Controllori SmartGuard 600

Manuale dell'utente

Numeri di catalogo 1752-L24BBB, 1752-L24BBBE

ALLEN-BRADLEY • ROCKWELL SOFTWARE

Rockwell Automation

Importanti informazioni per l'utente

Le apparecchiature a stato solido hanno caratteristiche funzionali che differiscono da quelle delle apparecchiature elettromeccaniche. Il manuale Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (pubblicazione SGI-1.1 disponibile presso l'ufficio vendite Rockwell Automation di zona oppure online all'indirizzo http://literature.rockwellautomation.com) descrive alcune importanti differenze tra le apparecchiature a stato solido e i dispositivi elettromeccanici cablati. A causa di queste differenze, e anche per la grande varietà di usi cui sono destinate le apparecchiature a stato solido, tutti i responsabili per l'utilizzo di questa apparecchiatura devono accertarsi che ciascuna applicazione sia idonea all'utilizzo previsto.

In nessun caso Rockwell Automation, Inc. sarà ritenuta responsabile per danni indiretti o consequenziali risultanti dall'uso o dall'applicazione dell'apparecchiatura.

Gli esempi e gli schemi contenuti nel presente manuale sono riportati a puro scopo illustrativo. A causa delle molte variabili e dei numerosi requisiti associati ad ogni particolare installazione, Rockwell Automation Inc. non può assumersi alcuna responsabilità civile o penale per l'uso effettivo basato su tali esempi e schemi.

Rockwell Automation, Inc. non si assume alcuna responsabilità sui brevetti in relazione all'uso di informazioni, circuiti elettrici, apparecchiature o software descritti nel presente manuale.

Si vieta la riproduzione, parziale o totale, del contenuto del presente manuale senza previo consenso scritto di Rockwell Automation, Inc.

Nel presente manuale, quando risulta necessario, vengono utilizzate note che hanno lo scopo di evidenziare considerazioni in materia di sicurezza.

AVVISO	Identifica informazioni sulle pratiche o circostanze che possono causare un'esplosione in un ambiente pericoloso con possibili conseguenti lesioni personali o morte, danni materiali e perdita economica.
IMPORTANTE	Identifica informazioni critiche per una corretta applicazione e comprensione del prodotto.
ATTENZIONE	Identifica le informazioni sulle pratiche o circostanze che possono determinare lesioni personali o morte, danni materiali o perdita economica. Gli avvisi di attenzione consentono di identificare ed evitare un pericolo e riconoscerne le conseguenze.
PERICOLO DI FOLGORAZIONE	È possibile che sopra o all'interno dell'apparecchiatura, ad esempio un azionamento o un motore, siano presenti etichette che avvisano gli utenti della presenza di tensioni pericolose.
PERICOLO DI USTIONI	È possibile che sopra o all'interno dell'apparecchiatura, ad esempio un azionamento o un motore, siano presenti etichette che avvisano gli utenti che le superfici potrebbero raggiungere temperature pericolose.

Allen-Bradley, Rockwell Automation, SmartGuard, Logix, ControlLogix, Guard I/O, POINT I/O, RSLogix 5000, RSNetWorx for DeviceNet, RSLinx e TechConnect sono marchi commerciali di Rockwell Automation, Inc.

I marchi commerciali che non appartengono a Rockwell Automation sono di proprietà delle rispettive società.

Le informazioni che seguono riepilogano le modifiche apportate a questo manuale dall'ultima stampa.

Argomento	**Pagina**
Aggiunta del controllore 1752-L24BBBE	in tutto il manuale
Aggiunta della comunicazione Ethernet	28
Aggiunta della messa a terra del controllore 1752-L24BBBE	30
Aggiornamento della figura che mostra la connessione alla porta DeviceNet	32
Aggiunta della connessione alla porta Ethernet	33
Aggiornamento dell'esempio di cablaggio del pulsante di emergenza	38, 283
Aggiornamento dell'esempio di cablaggio dell'interblocco di sicurezza	38, 285
Aggiunta del capitolo "Configurazione della rete EtherNet/IP"	Capitolo 4
Aggiornamento della comunicazione DeviceNet	Capitolo 7
Aggiunta del capitolo "Configurazione del controllore per le comunicazioni EtherNet/IP"	Capitolo 8
Aggiunta della tabella dei messaggi di errore EtherNet/IP	186
Aggiornamento delle specifiche dei controllori	195
Aggiornamento delle tabelle degli indicatori di stato dei moduli	201
Aggiunta dell'identificazione degli errori EtherNet/IP	210
Aggiornamento degli esempi di cablaggio doppia zona	286
Aggiornamento degli esempi di cablaggio della pedana di sicurezza	288

Note:

Prefazione

Destinatari del manuale 13
Scopo del manuale 13
Risorse aggiuntive 13
Convenzioni utilizzate nel manuale 14

Capitolo 1

Panoramica

Introduzione 15
Informazioni sul controllore SmartGuard 600 15
Hardware 17
Comunicazione 20
Configurazione e programmazione 20
Monitoraggio degli errori e dello stato 20
Concetto di sicurezza del controllore 21
Risorsa aggiuntiva 21

Capitolo 2

Installazione e cablaggio del controllore SmartGuard 600

Introduzione 23
Informazioni generali sulla sicurezza 23
Indirizzo di nodo 26
Impostazione dell'indirizzo di nodo 26
Impostazione della velocità di comunicazione 27
Comunicazione DeviceNet 27
Comunicazione Ethernet 28
Montaggio del controllore SmartGuard 29
Messa a terra del controllore SmartGuard 30
Collegamento di un alimentatore 30
Realizzazione delle connessioni di comunicazione 31
Collegamento della porta DeviceNet 32
Collegamento alla porta USB 33
Connessione alla porta Ethernet 33
Cablaggio del controllore SmartGuard 600 34
Cablaggio dei dispositivi di ingresso 35
Cablaggio dei dispositivi di uscita 37
Esempi di cablaggio 38

Capitolo 3

Configurazione della rete DeviceNet

Introduzione 41
Collegamento di un computer alla rete DeviceNet 41
Configurazione di un driver per la rete 42
Verifica del funzionamento del driver 42
Messa in servizio di tutti i nodi 42
Esplorazione della rete 44
Autenticazione di configurazione 45
Ripristino di sicurezza (opzionale) 46
Impostazione delle password (opzionale) 47
Impostazione o modifica di una password 47
Password dimenticate 48

Capitolo 4

Configurazione della rete EtherNet/IP

Introduzione 51
Collegamento di un computer alla rete EtherNet/IP 51
Configurazione di un driver per la rete 52
Verifica del funzionamento del driver 52
Connessione del controllore SmartGuard 600 alla rete EtherNet/IP 53
Impostazione dell'indirizzo IP 53
Utilizzo del BOOTP per impostare l'indirizzo IP 54
Utilizzo della utility BOOTP di Rockwell 55
Utilizzo del software RSLinx per impostare l'indirizzo IP 57
Funzione di bridge tra le reti 59
Comunicazione da una rete EtherNet/IP ad una rete DeviceNet 60
Comunicazione tra la porta USB e rete EtherNet/IP 62

Capitolo 5

Gestione del numero della rete di sicurezza (SNN)

Introduzione 63
Formati del numero della rete di sicurezza (SNN) 63
Numero della rete di sicurezza basato sul tempo (consigliato) 64
Numero della rete di sicurezza (SNN) manuale 64
Assegnazione del numero della rete di sicurezza (SNN) 65
Automatico (basato sul tempo) 65
Manuale 65
Impostazione del numero della rete di sicurezza (SNN) in tutti i nodi di sicurezza 66
Numero della rete di sicurezza (SNN) non corrispondente 67
Modifiche del numero della rete di sicurezza (SNN) e dell'indirizzo di nodo 67

Capitolo 6

Configurazione dell'I/O locale

Introduzione 69
Configurazione degli ingressi di sicurezza locali 69
Esempio: canale di ingresso impostato su Test Pulse from Test Output 73
Regolazione automatica del tempo di ritardo all'eccitazione e alla diseccitazione 74
Configurazione delle uscite di test locali 74
Configurazione delle uscite di sicurezza locali 76

Capitolo 7

Configurazione del controllore per le comunicazioni DeviceNet

Introduzione 79
Configurazione del controllore come master di sicurezza 79
Configurazione delle destinazioni I/O CIP Safety sulla rete DeviceNet 80
Configurazione dei collegamenti I/O di sicurezza 83
Modifica di una connessione I/O 86
Configurazione del controllore come slave di sicurezza 90
Creazione di dati I/O slave di sicurezza 90

Utilizzo del profilo generico di sicurezza nel software RSLogix 5000 93
Interblocco di sicurezza tra due controllori SmartGuard 96
Configurazione del controllore come slave DeviceNet standard 98
Creazione di dati I/O slave standard. 98
Aggiunta di uno slave standard SmartGuard all'elenco dei dispositivi del master standard 102
Lettura e scrittura tra il controllore SmartGuard e un'interfaccia PanelView Plus. 103
Lettura dati BOOL dal controllore SmartGuard e loro visualizzazione sull'interfaccia PanelView Plus. 104
Configurazione dell'elenco di scansione dello scanner PanelView 106
Configurazione dello scanner RN10C DeviceNet 107
Lettura e scrittura tra il controllore SmartGuard e l'interfaccia PanelView Plus, simultaneamente 113
Configurazione dell'elenco di scansione dello scanner PanelView 116
Configurazione dello scanner RN10C DeviceNet 118
Configurazione dei dati scritti dall'interfaccia PanelView Plus nel controllore SmartGuard 119
Confronto tra COS e polling 123
Dimensioni massime della connessione 125

Capitolo 8

Configurazione del controllore per le comunicazioni EtherNet/IP

Introduzione. 127
Collegamenti multicast. 127
Configurazione I/O target nel software RSNetWorx for DeviceNet 128
Configurazione del controllore come slave mediante il profilo generico del software RSLogix 5000 132
Configurazione della comunicazione tra un terminale PanelView standard ed un controllore SmartGuard 600 su una rete EtherNet/IP 134

Capitolo 9

Impostazione delle modalità del controllore

Introduzione. 137
Impostazione della modalità di esecuzione automatica (opzionale) 137
Impostazione della modalità di comunicazione stand alone (opzionale) 138
Modifica della modalità del controllore. 139

Capitolo 10

Creazione di un programma applicativo

Introduzione. 141
Logic Editor 141
Principi di programmazione 142
Funzioni logiche e blocchi funzione 143
Tag di ingresso 143

Tag di uscita. 145
Funzione dei commenti I/O 146
Limitazioni di programmazione. 146
Creazione di un programma con blocchi funzione. 147
Aggiunta di un tag di ingresso o uscita 147
Aggiunta di un blocco funzione 147
Collegamento dei tag al blocco funzione 148
Modifica dei parametri del blocco funzione 148
Impostazioni degli ingressi o delle uscite 149
Selezione di punti di uscita opzionali 150
Commenti 150
Ricerca dei blocchi funzione con collegamenti aperti. 151
Programmazione su più pagine 152
Salvataggio del programma 153
Aggiornamento del programma. 153
Monitoraggio del programma online 154
Sequenza di esecuzione del programma 155
Blocchi funzione definiti dall'utente 156
Creazione di blocchi funzione definiti dall'utente 156
Protezione con password dei blocchi funzione definiti dall'utente 157
Riutilizzo dei file dei blocchi funzione definiti dall'utente 158
Precauzioni per il riutilizzo dei blocchi funzione definiti dall'utente 160
Risorse aggiuntive 160

Capitolo 11

Download e verifica

Introduzione. 161
Download della configurazione di DeviceNet 161
Verifica della configurazione DeviceNet Safety. 163
Avvio della procedura guidata Safety Device Verification Wizard 163
Determinazione della possibilità di verificare i dispositivi 164
Selezione dei dispositivi per la verifica 165
Revisione dei report di verifica del dispositivo di sicurezza. 167
Blocco di sicurezza dei dispositivi 168
Visualizzazione del riepilogo della procedura guidata Safety Device Verification Wizard 169

Capitolo 12

Monitoraggio dello stato e gestione degli errori

Introduzione. 171
Indicatori di stato 171
Display alfanumerico 172
Monitoraggio dell'ingresso di alimentazione I/O 173
Monitoraggio delle informazioni sulla manutenzione I/O. 174
Monitoraggio del contatore commutazioni off/on 174
Monitoraggio del tempo totale di funzionamento 174
Configurazione di una modalità di monitoraggio di manutenzione 175
Cancellazione dei valori di manutenzione. 176

Visualizzazione dei dati di stato I/O. 177
Dati di stato generale. 178
Stato degli ingressi locali. 179
Stato delle uscite locali 179
Stato dell'uscita di test o della spia di muting 179
Stato di collegamento del controllore (funzione di slave di sicurezza). 180
Categorie di errore 182
Tabella cronologica degli errori 183
Area di memoria della cronologia errori. 183
Visualizzazione della tabella cronologica degli errori per il controllore 1752-L24BBB. 183
Visualizzazione della tabella cronologica degli errori EtherNet/IP per il controllore 1752-L24BBBE 184
Tabella cronologica degli errori EtherNet. 185
Messaggi della cronologia errori e azioni correttive 186
Errori di download e azioni correttive 190
Errori di ripristino e azioni correttive. 192
Errori di modifica della modalità e azioni correttive 193

Appendice A

Specifiche dei controllori

Introduzione. 195
Caratteristiche tecniche generali 195
Specifiche ambientali 197
Certificazioni 199

Appendice B

Indicatori di stato

Introduzione. 201
Indicatori di stato del modulo 201
Identificazione degli errori tramite gli indicatori di stato del modulo ed il display alfanumerico. 206
Identificazione degli errori EtherNet/IP tramite gli indicatori di stato ed il display alfanumerico 210

Appendice C

Riferimento per i comandi delle funzioni logiche

Introduzione. 211
Istruzione NOT. 211
Diagramma dell'istruzione NOT. 211
Tabella verità dell'istruzione NOT 211
Istruzione AND. 212
Diagramma dell'istruzione AND. 212
Tabelle verità dell'istruzione AND 212
Istruzione OR. 214
Diagramma dell'istruzione OR. 214
Tabelle verità dell'istruzione OR. 214
Istruzione Exclusive OR 216
Diagramma dell'istruzione Exclusive OR 216
Tabella verità dell'istruzione Exclusive OR. 217
Istruzione Exclusive NOR. 217

Diagramma dell'istruzione Exclusive NOR. 217
Tabelle verità dell'istruzione Exclusive NOR 217
Istruzione Routing 218
Diagramma dell'istruzione Routing 218
Tabella verità dell'istruzione Routing. 218
Istruzione Reset Set Flip-flop (RS-FF). 218
Diagramma dell'istruzione Reset Set Flip-flop 218
Gestione degli errori dell'istruzione Reset Set Flip-flop. 219
Diagramma dei tempi dell'istruzione Reset Set Flip-flop. 219
Istruzione Multi-connector 219
Diagramma dell'istruzione Multi-connector 219
Tabella verità per l'istruzione Multi-connector 220
Istruzione Comparator 220
Diagramma dell'istruzione Comparator 221
Parametri dell'istruzione Comparator 221
Tabella verità per l'istruzione Comparator 222
Diagramma dei tempi dell'istruzione Comparator 223

Appendice D

Riferimento per i comandi dei blocchi funzione

Introduzione. 225
Blocco funzione Reset 225
Parametri del blocco funzione Reset 226
Diagramma dei tempi del blocco funzione Reset. 227
Blocco funzione Restart. 227
Parametri del blocco funzione Restart 228
Diagramma dei tempi del blocco funzione Restart 229
Emergency Stop (ESTOP) 229
Parametri del blocco funzione ESTOP 230
Tabelle verità per il blocco funzione ESTOP 231
Gestione degli errori del blocco funzione ESTOP. 231
Diagramma dei tempi del blocco funzione ESTOP 231
Blocco funzione LC (Light Curtain) 232
Parametri del blocco funzione Light Curtain 232
Tabelle verità per il blocco funzione Light Curtain 233
Gestione degli errori del blocco funzione LC 233
Diagramma dei tempi del blocco funzione Light Curtain. 234
Blocco funzione Safety Gate Monitoring 234
Uscite opzionali del blocco funzione Safety Gate Monitoring. . . . 234
Impostazione dell'uscita Presenza guasto del blocco funzione Safety Gate Monitoring 235
Test funzionali del blocco funzione Safety Gate Monitoring. 235
Parametri del blocco funzione Safety Gate Monitoring. 236
Tabelle verità per il blocco funzione Safety Gate Monitoring 236
Gestione degli errori del blocco funzione Safety Gate Monitoring 237
Diagramma dei tempi del blocco funzione Safety Gate Monitoring 238
Blocco funzione Two-hand Control 239
Uscite opzionali del blocco funzione Two-hand Control 239

Impostazione dell'uscita Presenza guasto del blocco funzione Two-hand Control ... 239
Parametri del blocco funzione Two-hand Control ... 240
Tabella verità per il blocco funzione Two-hand Control ... 240
Gestione degli errori del blocco funzione Two-hand Control ... 241
Diagramma dei tempi del blocco funzione Two-hand Control ... 241
Blocco funzione OFF-delay Timer ... 242
Diagramma dei tempi del blocco funzione OFF-delay Timer ... 242
Blocco funzione ON-delay Timer ... 242
Diagramma dei tempi del blocco funzione ON-delay Timer ... 243
Blocco funzione User Mode Switch ... 243
Uscite opzionali del blocco funzione User Mode Switch ... 243
Impostazione dell'uscita Presenza guasto del blocco funzione User Mode Switch ... 244
Tabella verità per il blocco funzione User Mode Switch ... 244
Gestione degli errori del blocco funzione User Mode Switch ... 244
Diagramma dei tempi del blocco funzione User Mode Switch ... 245
EDM (External Device Monitoring) ... 245
Uscite opzionali del blocco funzione EDM ... 246
Impostazione dell'uscita Presenza guasto del blocco funzione EDM ... 246
Parametro del blocco funzione EDM ... 246
Gestione degli errori del blocco funzione EDM ... 246
Diagramma dei tempi del blocco funzione EDM ... 247
Muting ... 247
Parametri del blocco funzione Muting ... 248
Uscite opzionali del blocco funzione Muting ... 249
Impostazione dell'uscita Presenza guasto del blocco funzione Muting ... 249
Gestione degli errori del blocco funzione Muting ... 249
Dettagli sulla funzione Muting ... 250
Esempio: muting in parallelo con 2 sensori ... 251
Esempio: rilevamento posizione ... 259
Esempio: funzione di override ... 261
Enable switch ... 264
Parametri del blocco funzione Enable Switch ... 265
Uscite opzionali ... 265
Impostazione dell'uscita Presenza guasto ... 265
Gestione degli errori del blocco funzione Enable Switch ... 266
Diagrammi dei tempi del blocco funzione Enable Switch ... 266
Pulse Generator ... 267
Parametri del blocco funzione Pulse Generator ... 267
Diagramma dei tempi del blocco funzione Pulse Generator ... 267
Counter ... 268
Parametri del blocco funzione Counter ... 268
Condizione di ripristino ... 268
Tipo di conteggio ... 269
Diagramma dei tempi del blocco funzione Counter ... 269

Appendice E

Messaggi espliciti

Introduzione 271
Ricezione di messaggi espliciti 271
Formato del comando 271
Formato della risposta 272
Formato della risposta di errore 273
Esempio di messaggio di lettura da un controllore GuardLogix 274
Invio di messaggi espliciti 274
Restrizioni relative all'invio di messaggi espliciti 275
Accesso ai parametri del controllore utilizzando i messaggi espliciti DeviceNet 276

Appendice F

Esempi di applicazione e di configurazione

Introduzione 283
Applicazione di arresto d'emergenza 283
Applicazione di interblocco di sicurezza con ripristino automatico 285
Applicazione di interblocco di sicurezza a zona duale con interruttore di emergenza con ripristino manuale 286
Applicazione con pedane di sicurezza 288
Applicazione con barriera fotoelettrica 290

Glossario

Index

Leggere questa prefazione per avere una panoramica completa del manuale. Vengono fornite informazioni sui seguenti argomenti:

- destinatari del manuale
- scopo del manuale
- risorse aggiuntive
- convenzioni utilizzate nel manuale

Destinatari del manuale

Utilizzare il presente manuale se si è responsabili della progettazione, installazione, programmazione o ricerca guasti relativi a sistemi di controllo che utilizzano controllori SmartGuard 600.

È necessario avere una conoscenza di base dei circuiti elettrici ed esperienza con la logica a relè. Sono inoltre richieste formazione ed esperienza per la creazione, l'utilizzo e la manutenzione dei sistemi di sicurezza.

Scopo del manuale

Il presente manuale fornisce informazioni dettagliate per l'utilizzo dei controllori SmartGuard 600. Vengono descritte procedure specifiche per la configurazione, il funzionamento e la ricerca guasti del controllore SmartGuard 600.

Risorse aggiuntive

Nella tabella vengono elencate le pubblicazioni che contengono informazioni importanti sui sistemi del controllore SmartGuard 600.

Risorsa	Descrizione
Istruzioni di installazione "Controllore SmartGuard 600", pubblicazione 1752-IN001B-IT-P	Informazioni sull'installazione e il cablaggio del controllore SmartGuard 600
Manuale di riferimento per la sicurezza "Controllori SmartGuard 600", pubblicazione 1752-RM001B-IT-P	Informazioni dettagliate sui requisiti per la conformità SIL 3 del sistema del controllore SmartGuard
Istruzioni per l'installazione Moduli I/O di sicurezza per DeviceNet, pubblicazione 1791DS-IN001C-IT-P	Informazioni sull'installazione dei moduli Guard I/O DeviceNet Safety
Guard I/O DeviceNet Safety Modules User Manual, pubblicazione 1791DS-UM001	Informazioni sull'utilizzo dei moduli Guard I/O DeviceNet Safety
DeviceNet Media Design Installation Guide, pubblicazione DNET-UM072	Informazioni sulla pianificazione della rete EtherNet/IP

Le pubblicazioni possono essere visualizzate o scaricate all'indirizzo http://literature.rockwellautomation.com. Per ordinare copie cartacee dei documenti tecnici, rivolgersi al distributore o al rappresentante Rockwell Automation di zona.

Convenzioni utilizzate nel manuale

Nel manuale, sono state utilizzate le seguenti convenzioni:

- Gli elenchi puntati, come questo, contengono informazioni, non passi operativi.
- Gli elenchi numerati contengono passi in sequenza o informazioni gerarchiche.

Panoramica

Introduzione

Argomento	Pagina
Informazioni sul controllore SmartGuard 600	15
Concetto di sicurezza del controllore	21
Risorsa aggiuntiva	21

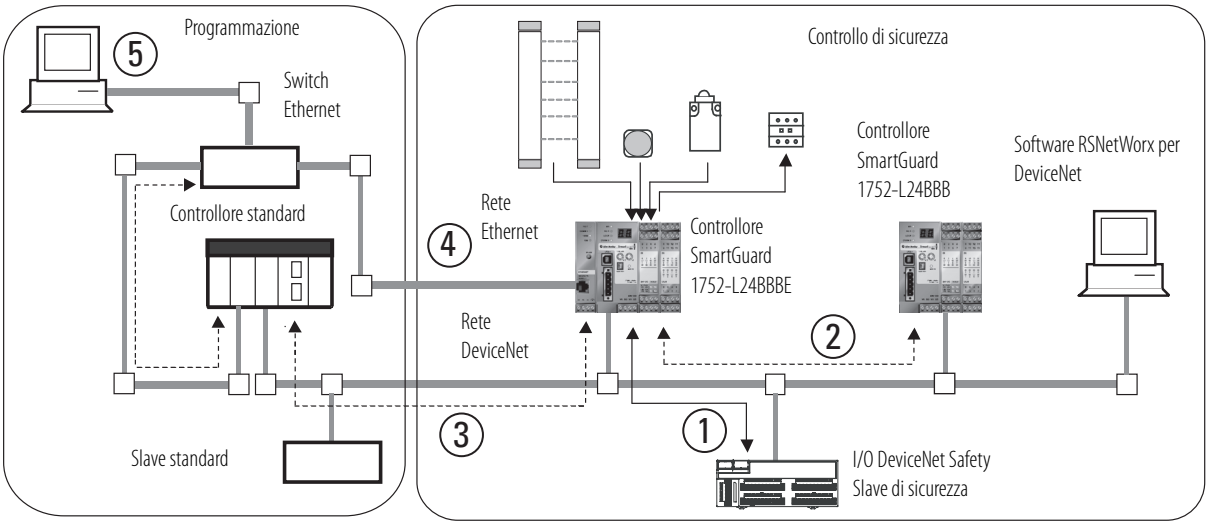
Informazioni sul controllore SmartGuard 600

I controllori SmartGuard 600 (numeri di catalogo 1752-L24BBB e 1752-L24BBBE) sono sistemi elettronici programmabili dotati di 16 ingressi digitali, 8 uscite digitali, 4 sorgenti ad impulsi di prova e connessioni per la comunicazione USB e DeviceNet. Inoltre, il controllore 1752-L24BBBE offre connettività EtherNet/IP.

Il controllore SmartGuard 600 supporta le comunicazioni standard e CIP Safety sulle reti DeviceNet e supporta la comunicazione CIP standard sulle reti EtherNet/IP.

Il controllore SmartGuard 600 è di tipo approvato e certificato per l'utilizzo in applicazioni di sicurezza fino al livello SIL (Safety Integrity Level) 3 incluso, conformemente alla norma IEC 61508, livello prestazionale PL(e) secondo la norma ISO 13849-1 e in applicazioni fino alla categoria CAT 4 inclusa, secondo la norma EN 954-1.

Esempio di sistema di controllo di sicurezza del controllore SmartGuard 600

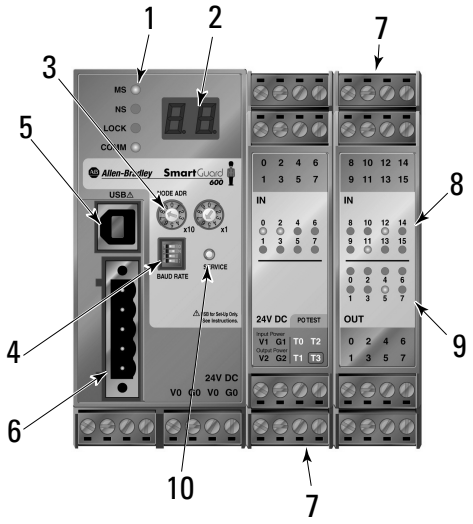


Numero	Descrizione
1	Come master di sicurezza DeviceNet, il controllore SmartGuard 600 può controllare fino a 32 moduli Guard I/O. Questi moduli 1791DS e 1732DS sono gli stessi moduli I/O di sicurezza distribuiti utilizzati con i controllori GuardLogix.
2	Come slave di sicurezza DeviceNet, il controllore SmartGuard 600 appare come un I/O di sicurezza distribuito ad un master di sicurezza. Un controllore GuardLogix o un altro master di sicurezza SmartGuard può leggere e scrivere dati di sicurezza sul controllore slave SmartGuard. Questo permette di realizzare il controllo di sicurezza distribuito mediante l'interblocco di più controllori attraverso CIP Safety su reti DeviceNet.
3	Come slave standard DeviceNet, il controllore SmartGuard 600 può fungere da modulo I/O distribuito standard e rispondere a messaggi espliciti in modo che i master DeviceNet standard, come i controllori ControlLogix, SLC 500 o PLC-5 o un'interfaccia operatore possano leggere e scrivere informazioni dal/nel controllore SmartGuard 600. Questo facilita il coordinamento con applicazioni PLC standard, compresa la visualizzazione delle informazioni del sistema di sicurezza su un'interfaccia operatore.
4	Come target standard EtherNet/IP, il controllore SmartGuard 600 comunica con un'origine standard Ethernet/IP, quale un controllore CompactLogix o MicroLogix o un dispositivo di interfaccia operatore. Il controllore SmartGuard non supporta la comunicazione CIP Safety su EtherNet/IP. Di conseguenza, il controllore SmartGuard non può controllare moduli di sicurezza 1791ES. Tutto il controllo di sicurezza deve avvenire sulla rete DeviceNet come illustrato ai punti 1 e 2 sopra.
5	Come bridge limitato EtherNet/IP, il controllore SmartGuard 600 consente di collegare in ponte a DeviceNet gli strumenti di programmazione, per visualizzare e programmare il controllore SmartGuard 600 e configurare altri dispositivi DeviceNet.

Hardware

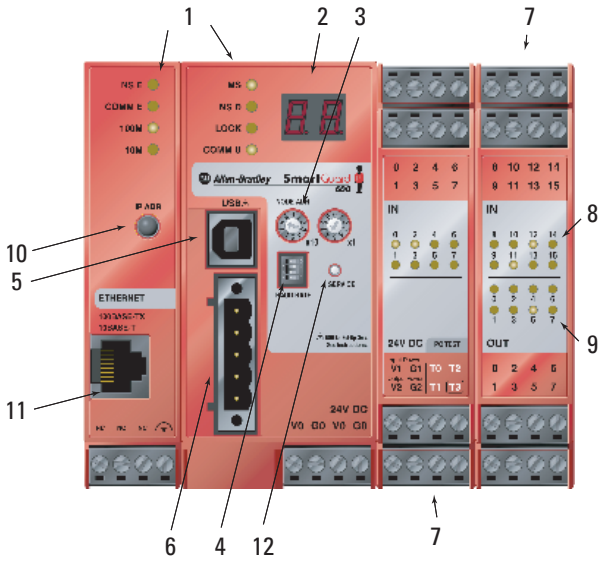
Il controllore SmartGuard 600 (numeri di catalogo 1752-L24BBB e 1752-L24BBBE) è dotato di 16 ingressi digitali, 8 uscite digitali, 4 sorgenti di test a impulsi e collegamenti per il protocollo USB e DeviceNet Safety. Inoltre, il controllore 1752-L24BBBE offre connettività EtherNet/IP.

Caratteristiche del controllore SmartGuard 600 (numero di catalogo 1752-L24BBB)



Numero	Caratteristica
1	Indicatori di stato del modulo
2	Display alfanumerico
3	Selettori di indirizzo di nodo
4	Selettori della velocità di trasmissione
5	Porta USB
6	Connettore di comunicazione DeviceNet
7	Connettori terminali
8	Indicatori di stato ingressi
9	Indicatori di stato uscite
10	Pulsante di servizio

Caratteristiche del controllore SmartGuard 600 (numero di catalogo 1752-L24BBBE)



Numero	Caratteristica
1	Indicatori di stato del modulo
2	Display alfanumerico
3	Selettori di indirizzo di nodo
4	Selettori della velocità di trasmissione
5	Porta USB
6	Connettore di comunicazione DeviceNet
7	Connettori terminali
8	Indicatori di stato ingressi
9	Indicatori di stato uscite
10	Pulsante di visualizzazione indirizzo IP
11	Connettore Ethernet
12	Pulsante di servizio

Ingressi di sicurezza

Il controllore è dotato di 16 ingressi di sicurezza locali che supportano le funzionalità descritte di seguito.

- Diagnosi dei circuiti di ingresso – È possibile utilizzare le sorgenti di test a impulsi per il monitoraggio dei circuiti interni, dei dispositivi esterni e del cablaggio esterno.
- Ritardi all'eccitazione e alla diseccitazione dell'ingresso – È possibile impostare dei filtri per il tempo di ingresso, compresi tra 0 e 126 ms in multipli della durata del ciclo del controllore. L'impostazione di ritardi all'eccitazione e alla diseccitazione dell'ingresso consente di ridurre l'influenza di chattering (oscillazioni) e dei disturbi esterni.
- Modalità doppio canale – È possibile impostare la modalità a doppio canale per coppie di ingressi locali associate. Se è stata impostata la modalità Canale duale, è possibile valutare le discrepanze temporali nelle modifiche di dati o nei segnali di ingresso tra due ingressi locali accoppiati.

Uscite di sicurezza

Il controllore è dotato di otto uscite di sicurezza locali che supportano le funzionalità descritte di seguito.

- Diagnosi del circuito di uscita – È possibile utilizzare impulsi di test per monitorare i circuiti interni, i dispositivi esterni e il cablaggio esterno del controllore.
- Rilevamento e protezione da sovracorrente – Per proteggere il circuito elettrico, l'uscita viene bloccata in caso di rilevamento di sovracorrente.
- Modalità Canale duale – È possibile impostare lo stato di sicurezza per entrambe le uscite accoppiate in caso di errore in una delle uscite locali accoppiate, indipendentemente dal programma utente.

Sorgenti di test a impulsi

Le quattro uscite di test indipendenti sono normalmente utilizzate insieme agli ingressi di sicurezza. Possono essere impostate anche per essere utilizzate come morsetti di uscita di segnale standard. Le uscite a impulsi di test supportano le seguenti funzionalità.

- Rilevamento e protezione da sovracorrente – Per proteggere il circuito elettrico, l'uscita viene bloccata in caso di rilevamento di sovracorrente.
- Rilevamento di corrente per spia di muting – È possibile rilevare disconnessioni solo per il morsetto T3.

Comunicazione

Il controllore può fungere da master o slave di sicurezza DeviceNet, da slave standard DeviceNet o da controllore stand alone quando le comunicazioni DeviceNet sono disabilitate. Un unico controllore può funzionare simultaneamente come master di sicurezza, slave di sicurezza e slave standard.

È possibile utilizzare i messaggi espliciti per leggere le informazioni di stato del controllore. Il programma utente può essere configurato per inviare messaggi espliciti. I messaggi possono essere inviati tra le reti DeviceNet e EtherNet/IP.

La porta USB può essere utilizzata per programmare il controllore SmartGuard e configurare i dispositivi di rete DeviceNet. SmartGuard fornisce funzionalità di tipo pass-through limitate da USB a DeviceNet, a scopo di programmazione e configurazione. Se utilizzato in modalità stand alone, il controllore comunica con il software di configurazione tramite USB.

Configurazione e programmazione

Utilizzare il software RSNetWorx for DeviceNet, versione 8.0 (minimo) o successiva (versione 9.1 raccomandata), per configurare, programmare e monitorare lo stato del controllore 1752-L24BBB. Utilizzare il software RSNetWorx for DeviceNet, versione 9.1 o successiva, per configurare, programmare e monitorare lo stato del controllore 1752-L24BBBE. Con il software RSNetWorx for DeviceNet, è possibile configurare il controllore utilizzando la porta USB del controllore SmartGuard o tramite la rete DeviceNet o EtherNet/IP.

È necessario anche il software RSLinx, versione 2.55 o successiva, che consente di configurare un controllore 1752-L24BBBE su EtherNet/IP.

Lo strumento Logic Editor viene avviato dal software RSNetWorx per DeviceNet. Sono supportati le operazioni logiche di base, quali AND e OR, e i blocchi funzione, quali arresto di emergenza e barriera fotoelettrica. È possibile utilizzare fino a 254 funzioni logiche e blocchi funzione in massimo 32 pagine di programmazione. È possibile proteggere con password i dati di configurazione e i file di progetto.

Monitoraggio degli errori e dello stato

È possibile monitorare online le informazioni sullo stato interno e i dati I/O del controllore utilizzando il software RSNetWorx for DeviceNet con un collegamento di rete USB, DeviceNet o EtherNet/IP.

Gli indicatori di stato e il display alfanumerico sul controllore forniscono informazioni sullo stato o sugli errori. Quando il pulsante di servizio sul pannello frontale del controllore viene premuto, sul display alfanumerico vengono visualizzate, due alla volta, le cifre dell'autenticazione della configurazione di sicurezza del controllore, per un totale di dieci coppie di numeri.

Quando il pulsante di visualizzazione dell'indirizzo IP viene premuto per almeno 1 secondo, il display visualizza l'indirizzo EtherNet/IP impostato.

Gli errori rilevati dal controllore vengono inclusi in un registro cronologico degli errori e in un registro cronologico EtherNet/IP, insieme all'ora di rilevamento dell'errore (l'ora viene mostrata come tempo di funzionamento totale dall'accensione del controllore).

Concetto di sicurezza del controllore

Il controllore SmartGuard 600 è di tipo approvato e certificato per l'utilizzo in applicazioni di sicurezza fino al livello SIL (Safety Integrity Level) 3 incluso, conformemente alla norma IEC 61508, livello prestazionale PL(e) secondo la norma ISO 13849-1 e in applicazioni fino alla categoria CAT 4 inclusa, secondo la norma EN 954-1, in cui lo stato diseccitato è lo stato di sicurezza. I requisiti delle applicazioni di sicurezza includono la valutazione delle probabilità di guasto (PFD e PFH), i calcoli del tempo di reazione del sistema e i test di verifica funzionale conformi ai criteri SIL 3. Leggere, comprendere e rispettare questi requisiti prima di utilizzare un sistema di sicurezza SIL 3 o CAT 4 basato su un controllore SmartGuard 600.

Il controllore utilizza i seguenti meccanismi per supportare l'integrità dei dati di sicurezza.

- Numero della rete di sicurezza (SNN) – Un numero univoco che identifica la rete di sicurezza. I nodi CIP Safety devono avere un SNN e un indirizzo di rete DeviceNet esclusivo.
- Autenticazione di configurazione – Combinazione di numero ID, data e ora che identificano in modo univoco una configurazione specifica di un dispositivo di sicurezza.
- Blocco della configurazione (o blocco di sicurezza) – Dopo il download e la verifica dei dati di configurazione, è possibile bloccare la configurazione del controllore per impedirne la modifica.
- Protezione con password – La configurazione del controllore può essere protetta utilizzando una password opzionale. Se viene impostata una password, per eseguire le operazioni di download, blocco, sblocco, ripristino e modifica dello stato è richiesta una password.

È necessario creare e documentare una distinzione chiara, logica e visibile tra le parti di sicurezza e quelle standard dell'applicazione.

Risorsa aggiuntiva

Per informazioni sui requisiti dei sistemi di sicurezza SIL 3 e CAT 4, inclusi gli intervalli di test di verifica funzionale, il tempo di reazione del sistema e i valori PFD/PFH, consultare il Manuale di riferimento per la sicurezza Controllori SmartGuard 600, pubblicazione 1752-RM001B-IT-P.

Note:

Installazione e cablaggio del controllore SmartGuard 600

Introduzione

Argomento	Pagina
Informazioni generali sulla sicurezza	23
Indirizzo di nodo	26
Impostazione dell'indirizzo di nodo	26
Impostazione della velocità di comunicazione	27
Montaggio del controllore SmartGuard	29
Messa a terra del controllore SmartGuard	30
Collegamento di un alimentatore	30
Cablaggio del controllore SmartGuard 600	34

Informazioni generali sulla sicurezza

ATTENZIONE

Ambiente e custodia

Questa apparecchiatura può funzionare in ambienti industriali con Grado di inquinamento 2, in applicazioni di sovratensione di categoria II, (come definito nella pubblicazione IEC 60664-1) ad altitudine fino a 2000 metri senza declassamento.

Questa apparecchiatura è considerata un'apparecchiatura industriale di Gruppo 1, Classe A secondo la pubblicazione 11 dell'IEC/CISPR. Senza le dovute precauzioni, vi potrebbero essere potenziali difficoltà nell'assicurare la compatibilità elettromagnetica in altri ambienti a causa dei disturbi condotti e irradiati.

Questa apparecchiatura viene fornita come apparecchiatura di tipo aperto. Deve essere montata all'interno di una custodia adatta alle specifiche condizioni ambientali di utilizzo e progettata specificatamente per evitare lesioni al personale derivanti dall'accesso a parti in tensione. La custodia deve essere dotata di opportune proprietà ritardanti di fiamma per impedire o ridurre al minimo la propagazione del fuoco, in conformità alla classificazione 5VA, V2, V1, V0 (o equivalente), in caso di componenti non metallici. La parte interna della custodia deve essere accessibile solo mediante l'utilizzo di utensili. Le successive sezioni di questa pubblicazione possono contenere ulteriori informazioni circa specifici tipi di custodie richieste per la conformità alle certificazioni di sicurezza di alcuni prodotti.

Oltre alla presente pubblicazione, vedere anche:

- Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione Allen-Bradley 1770-4.1.
- Standard NEMA 250 e pubblicazione IEC 60529, se pertinente, per spiegazioni in merito ai gradi di protezione forniti dai diversi tipi di custodie.

Approvazione nordamericana per l'uso in aree pericolose

The following information applies when operating this equipment in hazardous locations	**Informations sur l'utilisation de cet équipement en environnements dangereux**
Products marked CL I, DIV 2, GP A, B, C, D are suitable for use in Class I Division 2 Groups A, B, C, D, Hazardous Locations and nonhazardous locations only. Each product is supplied with markings on the rating nameplate indicating the hazardous location temperature code. When combining products within a system, the most adverse temperature code (lowest T number) may be used to help determine the overall temperature code of the system. Combinations of equipment in your system are subject to investigation by the local Authority Having Jurisdiction at the time of installation.	Les produits marqués CL I, DIV 2, GP A, B, C, D ne conviennent qu'à une utilisation en environnements de Classe I Division 2 Groupes A, B, C, D dangereux et non dangereux. Chaque produit est livré avec des marquages sur sa plaque d'identification qui indiquent le code de température pour les environnements dangereux. Lorsque plusieurs produits sont combinés dans un système, le code de température le plus défavorable (code de température le plus faible) peut être utilisé pour déterminer le code de température global du système. Les combinaisons d'équipements dans le système sont sujettes à inspection par les autorités locales qualifiées au moment de l'installation.

	EXPLOSION HAZARD • Do not disconnect equipment unless power has been removed or the area is known to be nonhazardous. • Do not disconnect connections to this equipment unless power has been removed or the area is known to be nonhazardous. Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product. • Substitution of components may impair suitability for Class I, Division 2. • If this product contains batteries, they must only be changed in an area known to be nonhazardous.	**AVERTISSEMENT** 	**RISQUE D'EXPLOSION** • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher l'équipement. • Couper le courant ou s'assurer que l'environnement est classé non dangereux avant de débrancher les connecteurs. Fixer tous les connecteurs externes reliés à cet équipement à l'aide de vis, loquets coulissants, connecteurs filetés ou autres moyens fournis avec ce produit. • La substitution de composants peut rendre cet équipement inadapté à une utilisation en environnement de Classe I, Division 2. • S'assurer que l'environnement est classé non dangereux avant de changer les piles.

Per l'utilizzo di questa apparecchiatura in aree pericolose attenersi alle seguenti informazioni

I prodotti marcati "CL I, DIV 2, GP A, B, C, D" sono adatti esclusivamente all'uso in aree pericolose di Classe I Divisione 2 Gruppi A, B, C, D e in aree non pericolose. Ciascun prodotto viene fornito con targhetta dati di classificazione che indica il codice temperatura per area pericolosa. Quando si assemblano diversi prodotti in un sistema, il codice temperatura più conservativo (numero "T" più basso) può essere usato come ausilio per determinare il codice temperatura generale del sistema. L'utilizzo di apparecchiature diverse all'interno del sistema è soggetto a ispezione da parte delle autorità locali competenti al momento dell'installazione.

AVVISO 	**RISCHIO DI ESPLOSIONE** • Non scollegare le apparecchiature senza aver prima staccato l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso. • Non scollegare le connessioni senza aver prima staccato l'alimentazione oppure senza essere certi di operare in un ambiente non pericoloso. Fissare i collegamenti esterni a questa apparecchiatura utilizzando viti, fermi scorrevoli, connettori filettati o qualsiasi altro strumento fornito con il prodotto. • La sostituzione dei componenti può compromettere l'idoneità per gli ambienti della classe I, Divisione 2. • Se il prodotto contiene batterie, queste ultime devono essere sostituite soltanto in un ambiente assolutamente non pericoloso.

ATTENZIONE 	Sistemi elettronici programmabili di sicurezza (PES) Il personale responsabile dell'applicazione di sistemi elettronici programmabili di sicurezza deve conoscere i requisiti di sicurezza dell'applicazione del sistema e deve essere addestrato all'uso del sistema.

ATTENZIONE

Prevenzione delle scariche elettrostatiche

Questa apparecchiatura è sensibile alle scariche elettrostatiche che possono provocare danni interni ed impedire il normale funzionamento. Osservare le seguenti precauzioni quando si maneggia questa apparecchiatura.

- Toccare un oggetto collegato a terra per scaricare il potenziale elettrostatico.
- Indossare un braccialetto antistatico regolamentare.
- Non toccare i connettori o i pin sulle schede dei componenti.
- Non toccare i componenti dei circuiti all'interno dell'apparecchiatura.
- Se disponibile, utilizzare un'area protetta ESD.
- Quando non è utilizzata, riporre l'apparecchiatura in una custodia antistatica appropriata.

ATTENZIONE

Pellicola antipolvere

Non rimuovere la pellicola antipolvere finché non viene completato il montaggio e il cablaggio del controllore e del resto dell'apparecchiatura nei pressi del controllore.

Dopo il completamento del cablaggio, rimuovere la pellicola antipolvere. Se prima dell'utilizzo la pellicola non viene rimossa correttamente, il sistema potrebbe surriscaldarsi.

ATTENZIONE

Potrebbero verificarsi danni gravi a causa della perdita della funzione di sicurezza richiesta.

- Non utilizzare le uscite di test come uscite di sicurezza.
- Non utilizzare i dati I/O standard DeviceNet o i dati dei messaggi espliciti come dati di sicurezza.
- Non utilizzare gli indicatori di stato per le operazioni di sicurezza.
- Non collegare carichi oltre al valore nominale indicato per le uscite di sicurezza o le uscite di test.
- Cablare il controllore correttamente in modo che la linea a 24 V CC non entri in contatto accidentalmente con le uscite.
- Mettere a terra la linea 0 V dell'alimentatore per i dispositivi di uscita esterni in modo che non vengano attivati quando la linea di uscita di sicurezza o la linea di uscita di test viene collegata a terra.
- Non smontare, riparare o modificare il controllore, poiché potrebbe esserne compromessa la sicurezza.

Indirizzo di nodo

Per comunicare sulla rete DeviceNet, ogni dispositivo deve avere un proprio indirizzo. Osservare le seguenti raccomandazioni per l'assegnazione degli indirizzi ai dispositivi di rete.

Raccomandazioni per l'indirizzo di nodo

Assegnare a questo dispositivo	L'indirizzo	Note
Scanner	0	Se vengono utilizzati più scanner, assegnare gli indirizzi in sequenza iniziando dal più piccolo.
Qualsiasi dispositivo di rete, tranne lo scanner	1…61	Non è necessario che gli indirizzi siano sequenziali. La presenza di intervalli non ha alcun effetto sulle prestazioni e offre maggiore flessibilità nello sviluppo del sistema.
Workstation RSNetWorx per DeviceNet	62	Se un computer viene collegato direttamente alla rete DeviceNet, utilizzare l'indirizzo 62 per il computer o il dispositivo ponte/di collegamento.
Nessun dispositivo	63	Lasciare l'indirizzo 63 aperto. Si tratta del tipico punto di ingresso alla rete di un nodo non assegnato.

La rete DeviceNet standard assegna le priorità di comunicazione in base al numero di nodo del dispositivo. Più basso è il numero di nodo, maggiore sarà la priorità di comunicazione del dispositivo. La priorità risulta importante quando più nodi tentano di comunicare in rete contemporaneamente.

I nodi di sicurezza DeviceNet hanno un'ulteriore priorità di rete, indipendentemente dal numero di nodo. Le comunicazioni di sicurezza DeviceNet dei dispositivi con numeri di nodo inferiori hanno priorità sulle comunicazioni di sicurezza DeviceNet di altri dispositivi con numeri di nodo superiori.

Impostazione dell'indirizzo di nodo

Impostare l'indirizzo di nodo prima di montare il controllore.

IMPORTANTE

Spegnere l'alimentazione del controllore prima di impostare l'indirizzo di nodo o la velocità di comunicazione tramite i selettori.

Non modificare le impostazioni dei selettori mentre l'alimentatore è acceso. Il controllore rileverà l'operazione come una modifica della configurazione e passerà alla modalità Interruzione (ABORT).

Utilizzare un piccolo cacciavite a lama piatta per impostare l'indirizzo di nodo tramite i due selettori rotativi sul pannello frontale del controllore. Prestare molta attenzione in modo da non graffiare i selettori. Sono validi i valori da 00 a 63. L'impostazione di default è 63.

Attenersi alla procedura seguente per impostare l'indirizzo di nodo.

1. Impostare la prima cifra (decina) dell'indirizzo di nodo (decimale) ruotando il selettore rotativo di sinistra.

2. Impostare la seconda cifra (unità) ruotando il selettore rotativo di destra.

3. Per consentire l'impostazione dell'indirizzo di nodo con il software RSNetworx for DeviceNet, impostare i selettori rotativi su un valore compreso tra 64 e 99.

IMPORTANTE Se viene impostato lo stesso indirizzo di nodo per più nodi, si verifica un errore di duplicazione dell'indirizzo di nodo.

Impostazione della velocità di comunicazione

Impostare la velocità di comunicazione prima di montare il controllore.

IMPORTANTE Spegnere l'alimentazione del controllore prima di impostare l'indirizzo di nodo o la velocità di comunicazione tramite i selettori.

Non modificare le impostazioni dei selettori mentre l'alimentatore è acceso. Il controllore rileverà l'operazione come una modifica della configurazione e passerà alla modalità Interruzione (ABORT).

Comunicazione DeviceNet

La velocità di comunicazione di default per una rete DeviceNet è di 125 Kbps.

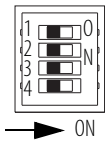
Se si sceglie di utilizzare una velocità di comunicazione differente, la lunghezza della linea dorsale e i tipi di cavo determinano la velocità di comunicazione supportata dall'applicazione.

Velocità di comunicazione e lunghezze del cavo per DeviceNet

Velocità di comunicazione	Distanza, max.			Lunghezza complessiva della linea di discesa
	Cavo piatto	Cavo spesso	Cavo sottile	
125 Kpbs	420 m	500 m	100 m	156 m
250 Kpbs	200 m	250 m	100 m	78 m
500 Kpbs	75 m	100 m	100 m	39 m

Impostare la velocità di comunicazione utilizzando il microinterruttore sul pannello frontale del controllore.

Microinterruttore della velocità di comunicazione



Impostazioni del microinterruttore

Pin del microinterruttore				Velocità di comunicazione
1	2	3	4	
OFF	OFF	OFF	OFF	125 Kbps
ON	OFF	OFF	OFF	250 Kbps
OFF	ON	OFF	OFF	500 Kbps
ON	ON	OFF	OFF	Impostata dal software
ON o OFF	ON o OFF	ON	OFF	Impostata dal software
ON o OFF	ON o OFF	ON o OFF	ON	Rilevamento automatico della velocità di trasmissione

IMPORTANTE Se viene modificata la velocità di comunicazione della rete, accertarsi che la nuova velocità di comunicazioni venga impostata per tutti i dispositivi. L'utilizzo di velocità di comunicazione diverse produce errori di comunicazione.

Se viene impostato il rilevamento automatico della velocità di trasmissione per alcuni dispositivi, è necessario configurare una velocità di comunicazione specifica per almeno uno degli altri dispositivi di rete. Se viene impostato il rilevamento automatico della velocità di trasmissione per tutti i dispositivi di rete, non sarà possibile stabilire una velocità di comunicazione, pertanto i dispositivi non potranno comunicare tra loro.

Comunicazione Ethernet

È consigliabile collegare il modulo alla rete attraverso un switch Ethernet da 100 Mbps che contribuirà a ridurre le collisioni e la perdita di pacchetti e ad incrementare la larghezza di banda.

Il controllore 1752-L24BBBE viene fornito con abilitazione BOOTP per l'impostazione dell'indirizzo IP. È possibile usare qualunque server BOOTP in commercio. In mancanza di supporto del server BOOTP sulla rete, scaricare il server BOOTP gratuito di Rockwell Automation dall'indirizzo http://www.rockwellautomation.com/rockwellsoftware/download/.

Per impostare l'indirizzo IP utilizzando l'utility BOOTP di Rockwell Automation, vedere a pagina 54.

La tabella che segue fornisce informazioni aggiuntive su EtherNet/IP.

Per informazioni dettagliate sulla comunicazione EtherNet/IP, consultare EtherNet/IP Performance and Application Solution, pubblicazione ENET-AP001.

Informazioni generali EtherNet/IP

Attributo	Valore
Numero di pacchetti CIP	2
Larghezza di banda ammissibile comunicazione unità	3000 pps(1)
Comunicazione messaggi espliciti	502 B(2)

(1) PPS è l'acronimo di Packets Per Second (pacchetti al secondo). Indica il numero di pacchetti inviati o ricevuti che possono essere elaborati ogni secondo.

(2) La lunghezza massima del messaggio per connessione classe 3 e connessione UCMM.

Montaggio del controllore SmartGuard

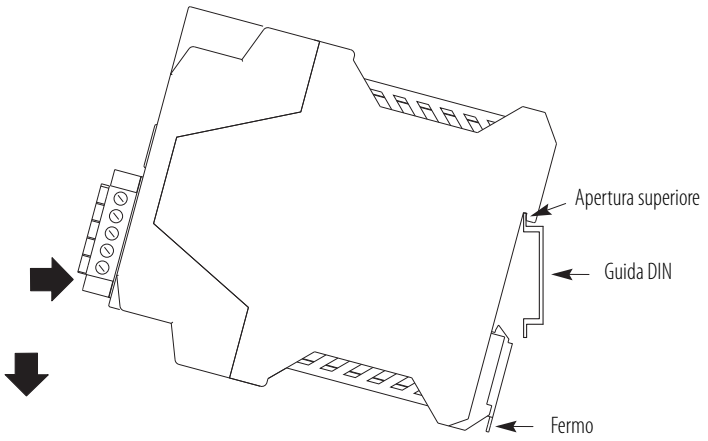
IMPORTANTE

Per un raffreddamento adeguato:

- montare il controllore su una guida DIN orizzontale. Non montare il controllore verticalmente
- garantire una distanza di almeno 50 mm sopra e sotto il controllore e 5 mm su ogni lato
- scegliere un'area ben ventilata oppure installare una ventola aggiuntiva.
- non montare il controllore su un dispositivo che produce calore.

Il controllore non può essere montato a pannello. Attenersi alla procedura seguente per montare il controllore su una guida DIN EN50022-35x7.5 o EN50022-35x15.

1. Agganciare lo slot superiore alla guida DIN.
2. Inserire la parte inferiore del controllore spingendo il controllore verso il basso, contro la parte superiore della guida.



3. Collegare i coperchi di protezione a ogni estremità della guida DIN.

Per rimuovere il controllore dalla guida DIN, utilizzare un cacciavite a lama piatta per abbassare il fermo ed estrarre il controllore dalla guida. Il controllore 1752-L24BBB ha un fermo ed il controllore 1752-L24BBBE ha due fermi sulla parte inferiore del controllore.

Messa a terra del controllore SmartGuard

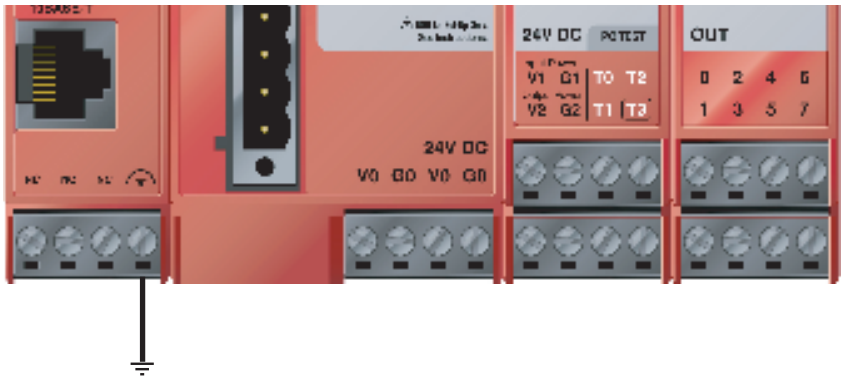
ATTENZIONE

Questo prodotto è messo a terra, attraverso la guida DIN, alla massa dello chassis. Utilizzare una guida DIN in acciaio cromato giallo e zincata per garantire la corretta messa a terra. L'uso di guide DIN di altri materiali (ad es. alluminio o plastica) che possono corrodersi, ossidarsi o sono cattivi conduttori, può comportare una messa a terra scorretta o intermittente. Fissare la guida DIN alla superficie di montaggio ogni 200 mm circa ed utilizzare correttamente gli ancoraggi terminali.

Fornire un percorso di massa adeguato per ogni dispositivo presente nell'applicazione. Collegare il controllore a terra secondo criteri di funzionalità tramite il collegamento di alimentazione V0/G0.

Inoltre, se si utilizza il controllore 1752-L24BBBE, è opportuno collegare il morsetto di terra Ethernet ad una messa a terra accettabile.

Messa a terra Ethernet



Per ulteriori informazioni, consultare il manuale Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1.

Collegamento di un alimentatore

Il controllore viene alimentato da una sorgente di alimentazione esterna in CC a 24 V. Il tempo di mantenimento dell'uscita deve essere uguale o superiore a 20 ms.

In conformità alla Direttiva CE sulla Bassa Tensione (LVD), i collegamenti e gli I/O DeviceNet devono essere alimentati da una sorgente CC a bassissima tensione di sicurezza (SELV) o a bassissima tensione di protezione (PELV).

In conformità alle norme UL, i collegamenti e gli I/O DeviceNet devono essere alimentati da sorgenti in CC con circuiti secondari isolati dal circuito primario tramite un isolamento doppio o rinforzato. L'alimentatore in CC deve soddisfare i requisiti previsti per i circuiti di Classe 2 o i circuiti a tensione/corrente limitata definiti nella norma UL 508.

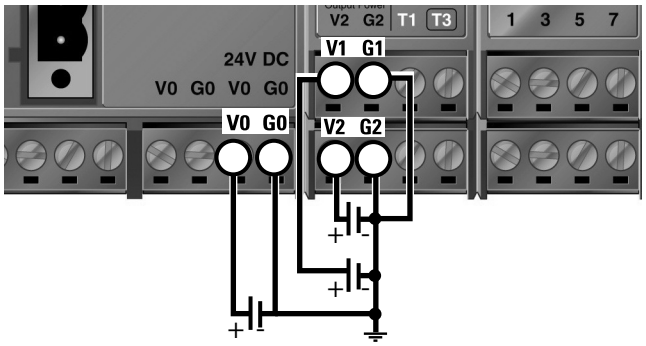
SUGGERIMENTO

I seguenti alimentatori Rockwell Automation della serie 1606 sono conformi all'alimentazione a bassissima tensione di sicurezza (SELV) o a bassissima tensione di protezione (PELV), inoltre soddisfano i requisiti di isolamento e del tempo di mantenimento dell'uscita del controllore SmartGuard 600:

- 1606-XLP30E
- 1606-XLP50E
- 1606-XLP50EZ
- 1606-XLP72E
- 1606-XLP95E
- 1606-XLDNET4
- 1606-XLSDNET4

Il controllore SmartGuard dispone di tre coppie di morsetti V/G che richiedono il collegamento dell'alimentazione. Sono presenti due coppie di morsetti V0/G0, ma poiché sono collegati internamente, è necessario collegarne una sola. È possibile utilizzare l'altra coppia per la distribuzione dell'alimentazione ad altri dispositivi.

Collegamenti dell'alimentatore



Realizzazione delle connessioni di comunicazione

AVVISO

Non collegare o scollegare il cavo di comunicazione prima di disattivare l'alimentazione del controllore o dei dispositivi di rete, poiché può verificarsi un arco elettrico. che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver staccato l'alimentazione o che l'area non sia pericolosa.

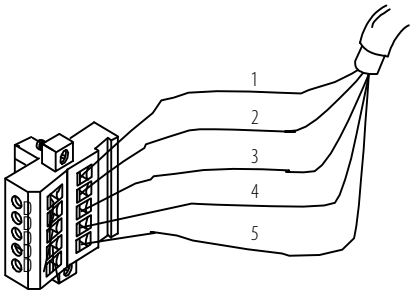
È possibile configurare la rete e il controllore sulla rete DeviceNet utilizzando una scheda 1784-PCD all'interno del PC e il software RSNetWorx forDeviceNet. È possibile anche configurare la rete e il controllore utilizzando la porta USB del controllore e il software RSNetWorx for DeviceNet. Inoltre, è possibile configurare il controllore usando il software RSNetWorx for DeviceNet, collegarlo alla porta EtherNet/IP e alla rete DeviceNet.

Collegamento della porta DeviceNet

Attenersi alla seguente procedura per effettuare il collegamento alla porta DeviceNet.

1. Collegare i fili al connettore in base ai colori sul connettore.

N. filo	Colore filo	Si collega a
V+	Rosso	V+
CAN H	Bianco	CAN H
Drain	–	Drenaggio
CAN L	Blu	CAN L
V-	Nero	V-



2. Collegare il connettore alla porta DeviceNet.

3. Stringere le viti a 0,25-0,3 N•m.

Per informazioni dettagliate sul collegamento DeviceNet, consultare il manuale DeviceNet Media Design Installation Guide, pubblicazione DNET-UM072. Consultare anche il manuale Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1.

Collegamento alla porta USB

Collegare il connettore di comunicazione USB al PC in uso per configurare la rete e il controllore con il software RSNetWorx for DeviceNet. Per effettuare il collegamento, utilizzare un cavo maschio-maschio USB-A a USB-B disponibile in commercio.

ATTENZIONE

Per ridurre potenziali disturbi elettromagnetici, la lunghezza del cavo USB deve essere inferiore a 3 m.

La porta USB deve essere utilizzata esclusivamente per la programmazione temporanea, e non per il collegamento permanente.

AVVISO

Se il cavo USB viene collegato o scollegato senza prima disattivare l'alimentazione del modulo o degli altri dispositivi di rete USB, può verificarsi un arco elettrico che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver staccato l'alimentazione o che l'area non sia pericolosa.

Connessione alla porta Ethernet

A seconda di dove si prevede di fare passare il cavo, è necessario selezionare il cavo più adatto all'ambiente. Negli ambienti industriali, il cavo schermato funziona meglio di quello non schermato. In particolare, se l'applicazione si trova in un ambiente molto disturbato o il cavo deve essere posato molto vicino a sorgenti di disturbo, è opportuno pianificare l'uso di cavi schermati.

Se l'applicazione include uno o più dei seguenti elementi, si dovrebbero considerare i cavi schermati:

- controllo saldatura a punti
- Centri controlo motori
- azionamenti da oltre 10 Hp
- processi di saldatura ad induzione
- vicinanza a emissionii RF di elevata potenza
- processi elettrostatici
- dispositivi a corrente elevata (superiori a 100 A)

IMPORTANTE

Le schermature svolgono un ruolo importante nel garantire al sistema l'immunità ai disturbi. Tuttavia, un cavo schermato installato in modo errato può provocare problemi a causa degli offset di tensione nel sistema di messa a terra. Per minimizzare gli effetti degli offset della tensione di massa, è necessario isolare la schermatura ad un'estremità del cavo. In questo caso, la schermatura dovrebbe essere isolata in corrispondenza del dispositivo, non dello switch.

Per collegare il controllore alla rete EtherNet/IP, utilizzare un connettore RJ45. Quando si collega il controllore SmartGuard ad uno switch o hub, usare un cavo Ethernet standard. Quando si collega il controllore SmartGuard direttamente al personal computer o ad una scheda NIC, utilizzare un cavo cross-over (null modem).

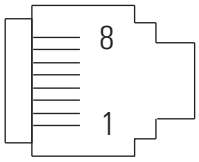
ATTENZIONE

La lunghezza del cavo tra l'hub ed i nodi deve essere inferiore a 100 m.

AVVISO

Se si collega o scollega il cavo EtherNet prima di disattivare l'alimentazione del controllore o dei dispositivi di rete, può verificarsi un arco elettrico. che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver staccato l'alimentazione o che l'area non sia pericolosa.

Piedinatura Ethernet

N. pin	Nome pin	Posizione pin
8	Non utilizzato	
7	Non utilizzato	
6	RD-	
5	Non utilizzato	
4	Non utilizzato	
3	RD+	
2	TD-	
1	TD+	

Cablaggio del controllore SmartGuard 600

Utilizzare cavi della lunghezza massima di 30 m.

Informazioni generali sul cablaggio

Attributo	Valore
Tipo di cavo	Rame
Categoria di cablaggio(1)	2 – sulle porte di alimentazione, segnale e comunicazione
Sezione del cavo	Per l'alimentatore e gli I/O, utilizzare un cavo a filo unico da 0,2-2,5 mm^2 (12-24 AWG) o un cavo flessibile a treccia da 0,34-1,5 mm^2 (16-22 AWG). Prima di effettuare il collegamento, preparare i cavi a treccia fissando le ghiere ai collari isolanti in plastica (conformi allo standard DIN 46228-4).
Coppia di serraggio dei morsetti I/O	0,56-0,79 N•m

(1) Utilizzare le informazioni fornite sulla categoria del conduttore per pianificare l'instradamento dei conduttori. Consultare Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1.

Descrizioni dei morsetti del controllore

Designazione morsetto	Descrizione
V0	Morsetto di alimentazione per circuito interno (logica).
G0	Morsetto di alimentazione per circuito interno (logica).
V1	Morsetto di alimentazione per circuiti di ingresso e uscite di test.
G1	Morsetto di alimentazione per circuiti di ingresso e uscite di test.
V2	Morsetto di alimentazione per uscite di sicurezza.
G2	Morsetto di alimentazione per uscite di sicurezza.
IN0-IN15	Morsetti per ingressi di sicurezza.
T0-T3	Morsetti di uscita di test che possono fornire sorgenti di test a impulsi per gli ingressi di sicurezza IN0-IN15. T3 può supportare anche il rilevamento dello scollegamento del cavo e di guasti della lampadina per alcuni carichi, ad esempio una spia di muting.
OUT0-OUT7	Morsetti per uscite di sicurezza.

AVVISO

Se i cavi vengono collegati o scollegati con l'alimentazione lato campo attivata, può verificarsi un arco elettrico che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver staccato l'alimentazione o che l'area non sia pericolosa.

AVVISO

Se la morsettiera rimovibile viene collegata o scollegata con l'alimentazione lato campo attivata, può verificarsi un arco elettrico che può causare esplosioni in installazioni che si trovano in aree pericolose. Prima di procedere, assicurarsi di aver staccato l'alimentazione o che l'area non sia pericolosa.

IMPORTANTE

Preparare i cavi a treccia fissando le ghiere ai collari isolanti in plastica (conformi allo standard DIN 46228-4). Ghiere con aspetto simile, ma non conformi, potrebbero non essere adatte alla morsettiera del controllore.

Cablaggio dei dispositivi di ingresso

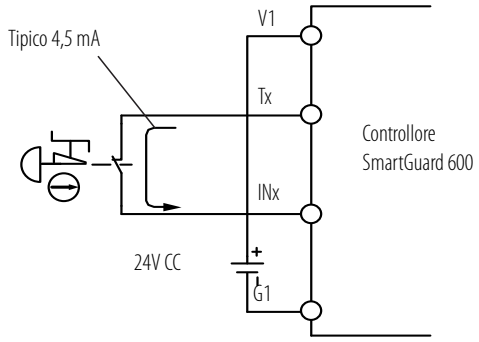
ATTENZIONE

Se viene fornita una tensione CC o CA non appropriata, potrebbero verificarsi perdite di sicurezza, danni al prodotto o lesioni gravi. Alimentare correttamente gli ingressi del controllore fornendo esclusivamente la tensione specificata.

I dispositivi di ingresso con uscite a contatti elettromeccanici, come i pulsanti di emergenza e gli interruttori di finecorsa di sicurezza, utilizzano sia un morsetto di ingresso di sicurezza sia un morsetto di uscita di test. Per questo, il circuito viene classificato come sistema di Categoria 4.

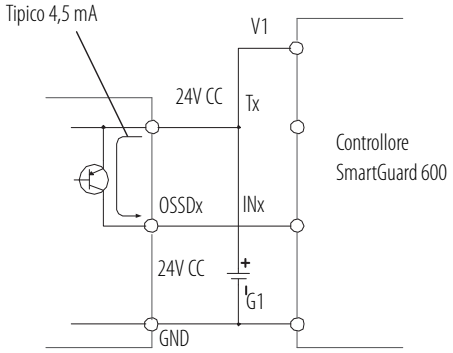
Quando i dispositivi di sicurezza sono collegati attraverso uscite di prova ad un circuito di ingresso sul controllore SmartGuard, è consigliabile che la lunghezza del cavo sia al massimo di 30 m.

Dispositivi di ingresso con uscite a contatti elettromeccanici



I dispositivi, quali le barriere fotoelettriche, con uscite a semiconduttore PNP sourcing di corrente inviano un segnale al morsetto di ingresso di sicurezza del controllore SmartGuard 600 e non utilizzano un'uscita di test.

Dispositivi di ingresso con uscite semiconduttori PNP



Cablaggio dei dispositivi di uscita

ATTENZIONE

Potrebbero verificarsi danni gravi a causa della perdita della sicurezza richiesta.

Non collegare carichi oltre al valore nominale indicato per le uscite di sicurezza o le uscite di test.

Non utilizzare le uscite di test come uscite di sicurezza.

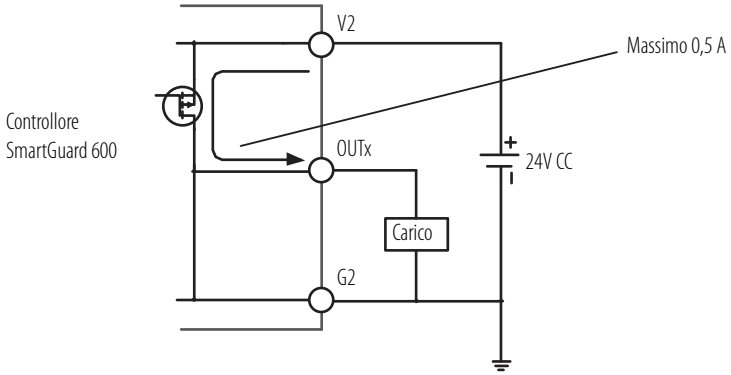
Cablare il controllore correttamente in modo che le linee in CC a 24 V non entrino in contatto con le uscite di sicurezza o di test.

Non alimentare i morsetti di uscita di test.

Mettere a terra la linea 0 V dell'alimentatore per i dispositivi di uscita esterni in modo che non vengano attivati quando la linea di uscita di sicurezza o la linea di uscita di test viene collegata a terra.

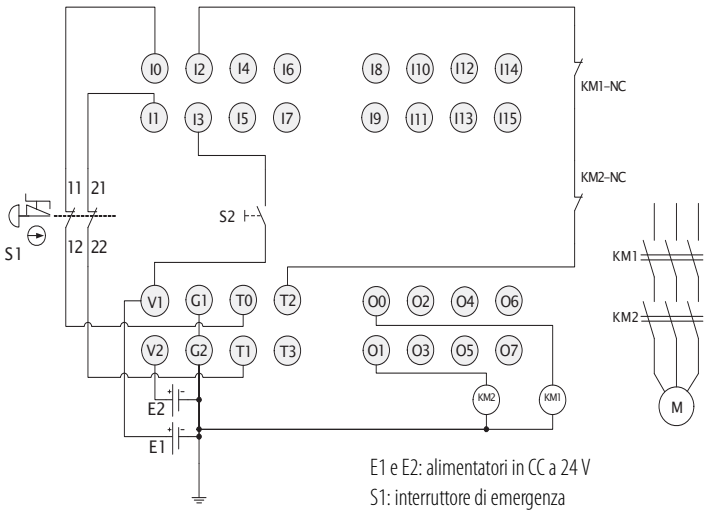
Separare i cavi I/O dalle linee ad alta tensione o a corrente elevata.

Cablaggio dei dispositivi di uscita



Esempi di cablaggio

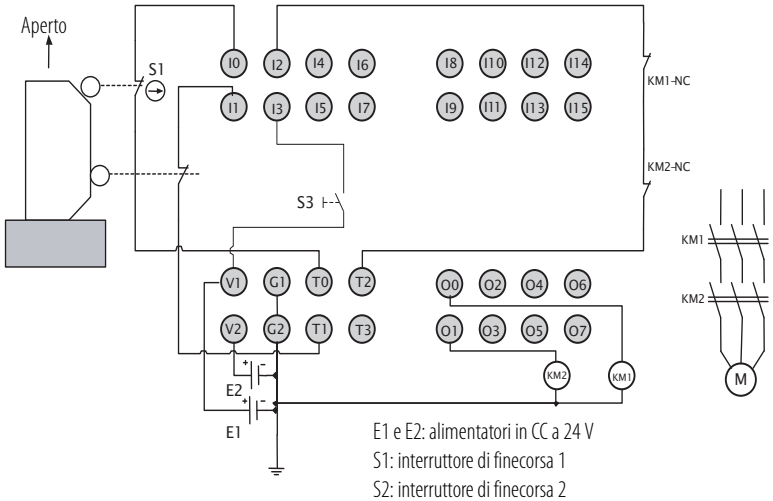
Arresto di emergenza



E1 e E2: alimentatori in CC a 24 V
S1: interruttore di emergenza
S2: interruttore di ripristino (contatto NA)
KM1 e KM2: contattori

Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

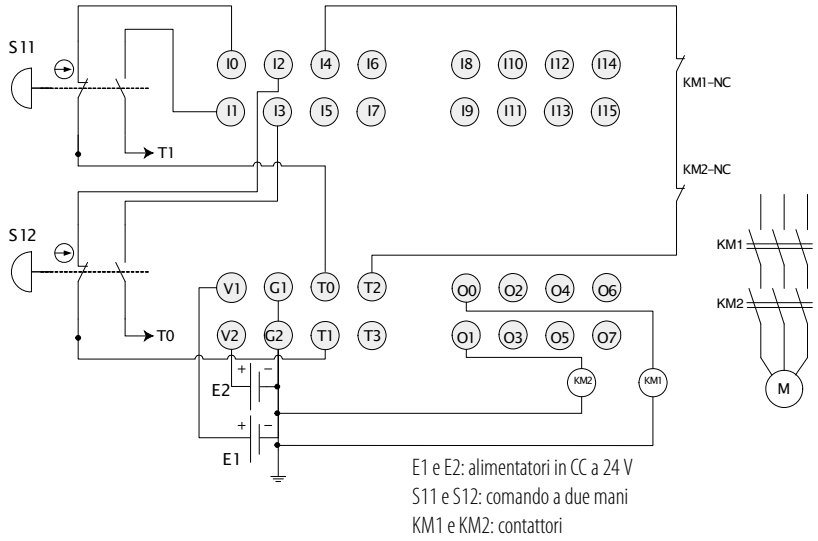
Interblocco di sicurezza



E1 e E2: alimentatori in CC a 24 V
S1: interruttore di finecorsa 1
S2: interruttore di finecorsa 2
S3: interruttore di ripristino
KM1 e KM2: contattori

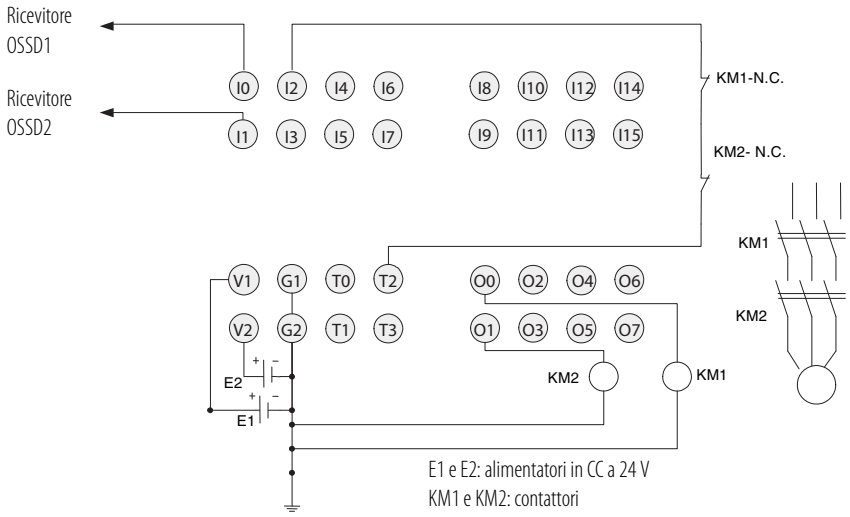
Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Comando a due mani



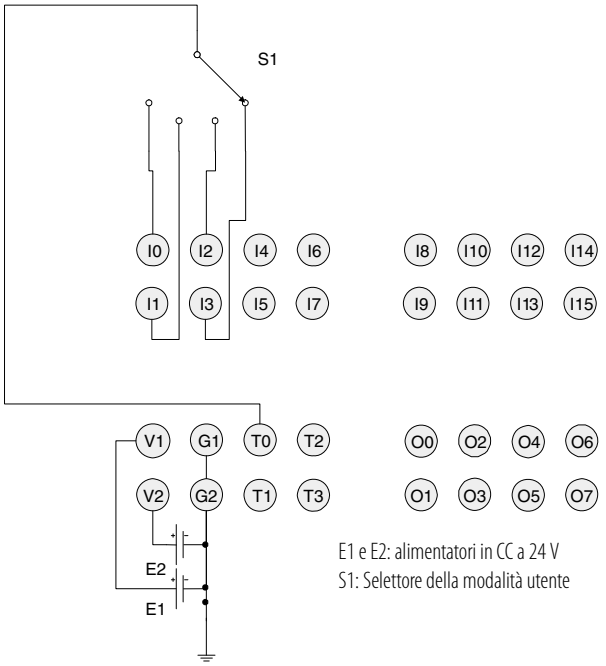
Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Barriera fotoelettrica



Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Selettore della modalità utente



E1 e E2: alimentatori in CC a 24 V
S1: Selettore della modalità utente

Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione della rete DeviceNet

Introduzione

Argomento	Pagina
Collegamento di un computer alla rete DeviceNet	41
Messa in servizio di tutti i nodi	42
Esplorazione della rete	44
Autenticazione di configurazione	45
Ripristino di sicurezza (opzionale)	46
Impostazione delle password (opzionale)	47

Collegamento di un computer alla rete DeviceNet

Per accedere a una rete, effettuare una delle seguenti operazioni:

- collegarsi direttamente alla rete
- collegarsi a una rete differente e individuare la rete desiderata tramite un dispositivo di collegamento.

SUGGERIMENTO È possibile esplorare le reti DeviceNet ed EtherNet/IP tramite la porta USB del controllore SmartGuard.

La funzionalità di bridging da SmartGuard USB a DeviceNet è limitata. Ad esempio, non è possibile configurare un modulo 1734-ADN o moduli POINT I/O. Inoltre, non è possibile configurare un modulo 1753-DNSI tramite il controllore SmartGuard. Per queste operazioni, utilizzare una scheda 1784-PCD.

Dopo avere scelto una rete:

- installare la scheda di comunicazione, se necessario
- determinare i parametri di rete per il computer, ad esempio l'indirizzo di rete
- collegare il computer alla rete utilizzando il cavo appropriato.

IMPORTANTE La prima volta che il controllore SmartGuard viene collegato al PC tramite la porta USB, Windows esegue la procedura di riconoscimento del dispositivo e richiede i driver USB. Il driver è disponibile sul CD RSLinx Classic nella cartella SmartGuardUSB-KernelDrivers.

Configurazione di un driver per la rete

1. Avviare il software RSLinx.
2. Fare clic su Configure Driver.
3. Dall'elenco a discesa Available Driver Types, aggiungere il driver per la rete.

Rete	Driver
RS-232	Dispositivi RS-232 DF1
EtherNet/IP	Dispositivi Ethernet
DeviceNet	Driver DeviceNet
USB	Driver SmartGuard USB

4. Configurare il driver.

   La configurazione delle impostazioni dipende dal tipo di rete scelta e dall'utilizzo di una scheda di comunicazione o di un modulo d'interfaccia.

Verifica del funzionamento del driver

1. Verificare la finestra di dialogo Configure Drivers per accertarsi che il driver sia in esecuzione.
2. Chiudere la finestra di dialogo.
3. Aprire la finestra di dialogo RSWho.
4. Fare doppio clic sul driver per visualizzare la rete.

Messa in servizio di tutti i nodi

Se l'indirizzo di nodo e la velocità di comunicazione dei dispositivi non sono stati specificamente impostati utilizzando i selettori hardware, è necessario mettere in servizio tutti i dispositivi mediante il software RSNetWorx for DeviceNet.

Prima di poter utilizzare lo strumento Node Commissioning di RSNetWorx per DeviceNet, il computer e i dispositivi DeviceNet devono essere collegati alla rete DeviceNet.

Utilizzare lo strumento Node Commissioning del software RSNetWorx per DeviceNet per impostare l'indirizzo di nodo e/o la velocità di comunicazione del controllore SmartGuard e degli altri dispositivi DeviceNet.

Seguire le regole generali riportate a pagina 26 per l'impostazione degli indirizzi di nodo per la rete DeviceNet.

IMPORTANTE Per consentire l'impostazione dell'indirizzo di nodo con lo strumento Node Commissioning del software RSNetWorx for DeviceNet, impostare il selettore rotativo dell'indirizzo di nodo sul controllore su un valore compreso tra 64 e 99.

Vedere pagina 26 per informazioni sull'impostazione dell'indirizzo di nodo utilizzando il selettore rotativo.

Per utilizzare lo strumento Node Commissioning, attenersi alla procedura seguente.

1. Nel software RSNetWorx for DeviceNet, selezionare Tools > Node Commissioning.
2. Fare clic su Browse nella finestra di dialogo Node Commissioning per selezionare un dispositivo esplorando la rete.

   Per raggiungere la porta DeviceNet, è possibile esplorare attraverso la porta USB SmartGuard o la porta Ethernet/IP.
3. Selezionare la rete DeviceNet nel riquadro di sinistra.
4. Selezionare il dispositivo da mettere in servizio nel riquadro di destra e fare clic su OK.
5. Modificare la velocità di comunicazione del dispositivo, se richiesto, selezionando il valore desiderato.

   IMPORTANTE La velocità di comunicazione del dispositivo non viene aggiornata finché il dispositivo non viene spento e riacceso o ripristinato.
6. Nella finestra di dialogo Node Commissioning, immettere il nuovo indirizzo del dispositivo e fare clic su Apply.

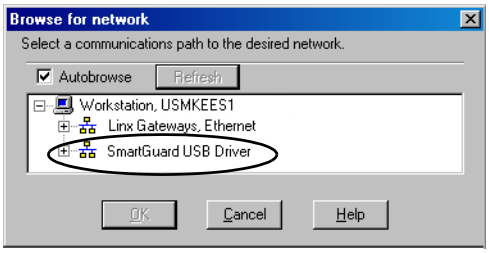
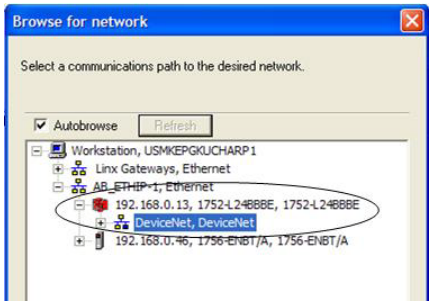
   Viene visualizzato un messaggio di conferma del completamento dell'operazione.

   IMPORTANTE Per modificare l'indirizzo di nodo di un dispositivo di sicurezza, è necessario prima ripristinare il numero della rete di sicurezza (SNN) in uno stato non inizializzato eseguendo un ripristino di sicurezza, come descritto a pagina 46.

Esplorazione della rete

Attenersi alla procedura seguente per esplorare la rete.

1. Determinare il tipo di collegamento.

Se viene utilizzato questo tipo di collegamento	Procedere come segue:
Rete DeviceNet	Andare al punto 2.
Porta USB	Attenersi alla procedura seguente per configurare un percorso alla rete DeviceNet. A. Dal menu Network, scegliere Properties. B. Nella finestra di dialogo DeviceNet, fare clic su Set Online Path. C. Nella finestra di dialogo Browse for Network, selezionare il percorso desiderato e fare clic su OK. 
Rete EtherNet/IP	Attenersi alla procedura seguente per configurare un percorso alla rete DeviceNet. A. Dal menu Network, scegliere Properties. B. Nella finestra di dialogo DeviceNet, fare clic su Set Online Path. C. Nella finestra di dialogo Browse for Network, selezionare il percorso desiderato e fare clic su OK. 

2. Fare clic sull'icona online .
3. Attendere il completamento dell'operazione di esplorazione della rete.

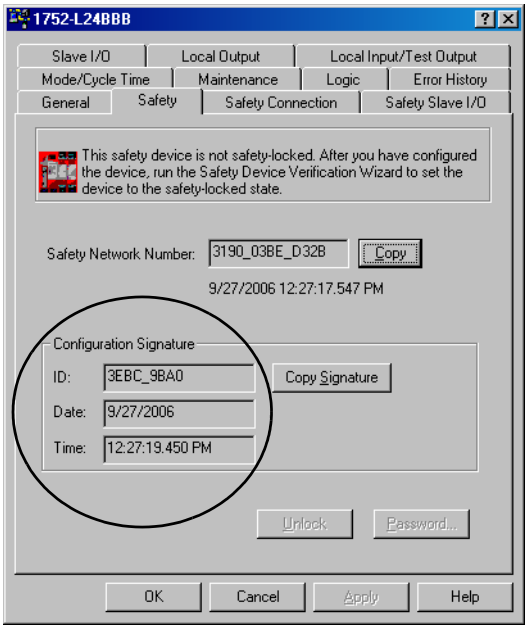
   Durante l'esplorazione della rete, tutti i dispositivi di rete vengono visualizzati nel software RSNetWorx per DeviceNet.
4. Verificare che tutti i nodi siano visualizzati.
5. Salvare il progetto nel software RSNetWorx per DeviceNet.

Autenticazione di configurazione

Ogni dispositivo di sicurezza presenta una autenticazione di configurazione univoca, che ne identifica la configurazione per verificare l'integrità dei dati di configurazione durante i download, il collegamento e la sostituzione dei moduli.

L'autenticazione di configurazione è costituita da numero ID, data e ora e viene impostata automaticamente dal software RSNetWorx per DeviceNet quando la configurazione del dispositivo viene aggiornata. L'autenticazione di configurazione viene riportata nella scheda Safety della finestra di dialogo Device Properties. Inoltre, viene visualizzata sul display alfanumerico, un carattere alla volta, quando viene premuto il pulsante di servizio.

Autenticazione di configurazione del controllore SmartGuard 600

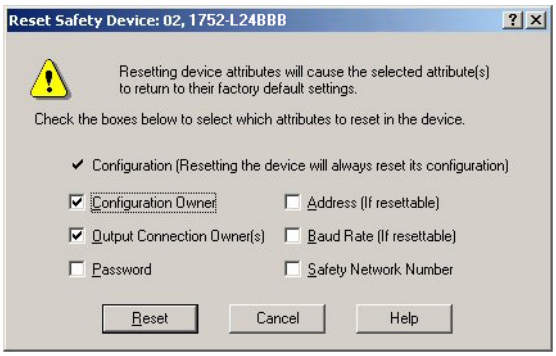


L'autenticazione di configurazione viene letta durante ogni esplorazione e ogni volta che viene avviata la finestra di dialogo Device Properties quando il software è in modalità Online. Il software RSNetWorx per DeviceNet confronta l'autenticazione della configurazione nel file di configurazione del dispositivo (offline) del software con l'autenticazione della configurazione del dispositivo online. Se le autenticazioni di configurazione non corrispondono, viene richiesto di caricare la configurazione del dispositivo online o di scaricare la configurazione del dispositivo software per risolvere il problema.

Ripristino di sicurezza (opzionale)

Se necessario, è possibile ripristinare gli attributi del dispositivo di sicurezza ripristinando i valori di default di fabbrica nella finestra di dialogo Reset Safety Device.

È possibile ripristinare gli attributi visualizzati nella finestra di dialogo Reset Safety Device selezionando le caselle di controllo corrispondenti. Se la casella di controllo di un attributo non viene selezionata, l'impostazione di tale attributo non viene modificata durante l'operazione di ripristino di sicurezza.



1. Aprire la finestra di dialogo Reset Safety Device facendo clic sul dispositivo nella vista grafica del software RSNetWorx for DeviceNet e selezionando Reset Safety Device dal menu Device.

2. Selezionare gli attributi da ripristinare.

Attributo	Modo di ripristino
Configurazione	La configurazione del dispositivo viene cancellata in seguito all'operazione di ripristino di sicurezza.
Configuration Owner	Selezionare questa casella di controllo per ripristinare il proprietario della configurazione del dispositivo. Per i controllori SmartGuard, il software di configurazione è sempre il proprietario della configurazione.
Output Connection Owner(s)	Selezionare questa casella di controllo per ripristinare tutti i proprietari dei collegamenti di uscita esistenti. Il successivo dispositivo che accede a un punto di collegamento di uscita in seguito al ripristino di sicurezza diventa il proprietario del collegamento di uscita.
Password	Selezionare questa casella di controllo per ripristinare la password del dispositivo. Per ripristinare una password dalla finestra di dialogo Reset Safety Device, è necessario conoscere la password corrente del dispositivo.
Address	Selezionare questa casella di controllo per ripristinare l'indirizzo di nodo del dispositivo configurato tramite software su 63. Se l'indirizzo di nodo è stato impostato utilizzando i selettori, l'operazione di ripristino non interessa l'indirizzo di nodo, che pertanto non viene modificato.
Baud Rate	Selezionare questa casella di controllo per ripristinare la velocità di comunicazione del dispositivo su 125 Kbps. Se la velocità di comunicazione del dispositivo è stata impostata utilizzando i selettori, l'operazione di ripristino non interessa la velocità di comunicazione, che pertanto non viene modificata.
Safety Network Number	Selezionare questa casella di controllo per ripristinare il numero della rete di sicurezza (SNN).

3. Fare clic su Reset.

Se il dispositivo è in blocco di sicurezza, è necessario prima sbloccarlo.

ATTENZIONE

Una volta sbloccato, il dispositivo non viene più ritenuto attendibile per l'esecuzione delle operazioni di sicurezza.

Testare e verificare il funzionamento del dispositivo, quindi eseguire la procedura guidata Safety Device Verification Wizard per il blocco di sicurezza prima di utilizzarlo in un'applicazione di sicurezza.

4. Quando richiesto, immettere la password, se ne è stata impostata una per il dispositivo.

Impostazione delle password (opzionale)

È possibile proteggere i dispositivi di sicurezza con una password per impedire che la configurazione del dispositivo venga modificata da personale non autorizzato. Se impostata, le seguenti operazioni richiederanno l'immissione della password.

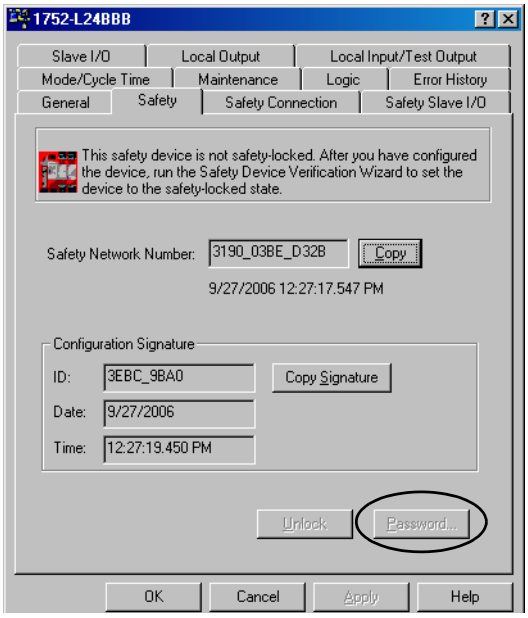
- Download
- Ripristino configurazione di sicurezza
- Blocco di sicurezza
- Sblocco

Impostazione o modifica di una password

Attenersi alla procedura seguente per impostare una password per un modulo.

1. Fare doppio clic sul modulo per aprire la finestra di dialogo Device Properties.
2. Selezionare la scheda Safety.

3. Fare clic su Password.



SUGGERIMENTO È anche possibile aprire la finestra di dialogo Set Device Password in uno dei seguenti modi:

- fare clic sul modulo e selezionare Set Password dal menu Device
- fare clic con il pulsante destro del mouse sul modulo e selezionare Set Password.

4. Immettere la vecchia password, se esistente.

5. Immettere e confermare la nuova password.

   Le password possono essere costituite da 1 a 40 caratteri, senza distinzione tra maiuscole e minuscole. È possibile utilizzare lettere, numeri e i seguenti simboli: ‘ ~ ! @ # $ % ^ & * ( ) _ + , – = { } | [ ] \ : ; ? / .

6. Fare clic su OK.

Password dimenticate

Se si dimentica la password, è possibile ripristinarla.

1. Nella scheda Safety della finestra di dialogo Device Properties, fare clic su Password per aprire la finestra di dialogo Set Device Password.

2. Fare clic su Reset Password.

3. Contattare l'assistenza tecnica Rockwell Automation e fornire il numero seriale e il codice di sicurezza del dispositivo riportati nella finestra di dialogo Reset Password.

4. Immettere nella finestra di dialogo Reset Device Password la password del fornitore ottenuta dall'assistenza tecnica Rockwell Automation, quindi fare clic su OK.

Note:

Configurazione della rete EtherNet/IP

Introduzione

Argomento	Pagina
Collegamento di un computer alla rete EtherNet/IP	51
Connessione del controllore SmartGuard 600 alla rete EtherNet/IP	53
Funzione di bridge tra le reti	59

Collegamento di un computer alla rete EtherNet/IP

Per accedere alla rete EtherNet/IP:

- collegarsi direttamente alla rete
- collegarsi a una rete differente e individuare la rete desiderata tramite un dispositivo di collegamento.

SUGGERIMENTO È possibile esplorare la rete EtherNet tramite la porta USB del controllore SmartGuard.

La funzione di bridge da SmartGuard USB a EtherNet è limitata.

Dopo avere scelto una rete:

- installare la scheda di comunicazione, se necessario
- determinare i parametri di rete per il computer, ad esempio l'indirizzo di rete
- collegare il computer alla rete utilizzando il cavo appropriato.

IMPORTANTE La prima volta che il controllore SmartGuard viene collegato al PC tramite la porta USB, il sistema operativo Windows esegue la procedura di riconoscimento del dispositivo e richiede i driver USB. Il driver è disponibile sul CD RSLinx Classic nella cartella SmartGuardUSB-KernelDrivers.

Configurazione di un driver per la rete

1. Avviare il software RSLinx.

   Perché il software RSLinx localizzi nuovi dispositivi sulla rete EtherNet/IP, il driver può essere configurato (opzione "Browse remote subnet") per cercare un indirizzo IP specifico e una maschera.

2. Fare clic su Configure Driver.

3. Dall'elenco a discesa Available Driver Types, selezionare il driver per la rete.

Rete	Driver
RS-232	Dispositivi RS-232 DF1
EtherNet/IP	Dispositivi Ethernet
DeviceNet	Driver EtherNet/IP
USB	Driver SmartGuard USB

4. Configurare il driver.

   La configurazione delle impostazioni dipende dal tipo di rete scelta e dall'utilizzo di una scheda di comunicazione o di un modulo d'interfaccia.

Verifica del funzionamento del driver

1. Verificare la finestra di dialogo Configure Drivers per accertarsi che il driver sia in esecuzione.

   SUGGERIMENTO È possibile configurare il driver utilizzando la selezione Remote Subnet ed impostando indirizzo IP e maschera sul valore del controllore SmartGuard. Questo permette al software RSLinx di trovare rapidamente il dispositivo.

2. Chiudere la finestra di dialogo.

3. Aprire la finestra di dialogo RSWho.

4. Fare doppio clic sul driver per visualizzare la rete.

Connessione del controllore SmartGuard 600 alla rete EtherNet/IP

IMPORTANTE I controllori SmartGuard non devono essere collegati direttamente alle reti non protette da intrusioni esterne. Ad esempio, non collegare il controllore SmartGuard 600 ad una rete Ethernet che non sia protetta con un firewall o altra misura di protezione.

Impostazione dell'indirizzo IP

Per configurare il controllore, definire indirizzo IP, maschera di sottorete e gateway.

Parametri EtherNet/IP

Parametro EtherNet/IP	Descrizione
IP Address	L'indirizzo IP identifica univocamente il controllore. L'indirizzo IP è in formato *xxx.xxx.xxx.xxx*. dove ogni *xxx* è un numero compreso tra 0 e 255. I seguenti valori riservati non possono essere utilizzati: • 127.0.0.1 • 0.0.0.0 • 255.255.255.255
Subnet Mask	L'indirizzamento di sottorete è un'estensione dello schema dell'indirizzo IP che permette ad un sito di usare un singolo ID di rete per diverse reti fisiche. L'instradamento all'esterno del sito continua dividendo l'indirizzo IP in un ID di rete e in un ID host tramite la classe. All'interno di un sito, la maschera di sottorete serve a suddividere l'indirizzo IP in un ID di rete personalizzato ed in un ID host. Di default, questo campo è impostato a 0.0.0.0. Se si modifica la maschera di sottorete di un controllore già configurato, è necessario spegnere e riaccendere perché la modifica abbia effetto.
Gateway	Un gateway collega le singole reti fisiche in un sistema di reti. Quando un nodo deve comunicare con un nodo di un'altra rete, il gateway trasferisce i dati tra le due reti. Di default, questo campo è impostato a 0.0.0.0.

È possibile configurare il controllore attraverso due opzioni; attraverso il software RSLinx Classic o attraverso una utility BOOTP. Vedere a pagina 54 per l'uso del BOOTP o a pagina 57 per l'uso del software RSLinx.

Utilizzo del BOOTP per impostare l'indirizzo IP

Il BOOTP (protocollo di bootstrap) è un protocollo a basso livello che i nodi TCP/IP usano per ottenere informazioni all'avvio. Un indirizzo IP non viene impostato fino al ricevimento di una risposta BOOTP. Il BOOTP consente di assegnare dinamicamente gli indirizzi IP ai processori sul collegamento Ethernet.

Per usare il BOOTP, sulla sottorete Ethernet locale deve esistere un server BOOTP. Il server è un computer che ha installato il software del server BOOTP e legge un file di testo contenente le informazioni di rete per i singoli nodi sulla rete.

Il file di configurazione BOOTP del sistema host deve essere aggiornato per rispondere alle richieste dal controllore SmartGuard. Nello stato di default (come fornito), il controllore SmartGuard richiede l'uso di un server BOOTP per impostare il suo indirizzo IP.

Vedere Impostazione dell'indirizzo IP per i parametri che devono essere configurati.

SUGGERIMENTO È possibile utilizzare qualunque server BOOTP in commercio. Se la rete non include il server BOOTP e si desidera configurare dinamicamente il controllore SmartGuard, è possibile scaricare il server BOOTP gratuito di Rockwell Automation all'indirizzo http://www.rockwellautomation.com/rockwellsoftware/download/.

Quando il BOOTP è abilitato, all'accensione si verifica quanto segue:

- Il processore trasmette un messaggio di richiesta BOOTP contenente il suo indirizzo hardware sulla rete o la sottorete locale.
- Il server BOOTP confronta l'indirizzo hardware con gli indirizzi nella sua tabella di ricerca.
- Il server BOOTP reinvia un messaggio al processore con l'indirizzo IP ed altre informazioni di rete che corrisponde all'indirizzo hardware ricevuto.

Con tutti gli indirizzi hardware e IP in una posizione, è possibile cambiare gli indirizzi IP nel file di configurazione BOOTP se la rete deve essere modificata.

La richiesta BOOTP può essere disabilitata azzerando il parametro BOOTP Enable nella scheda Port Configuration. Quando BOOTP Enable è azzerato (disabilitato), il controllore SmartGuard usa i dati di configurazione del canale esistente.

IMPORTANTE Quando il protocollo BOOTP viene utilizzato per impostare l'indirizzo IP in un controllore SmartGuard, il controllore SmartGuard deve ricevere un indirizzo IP iniziale dal server prima che il protocollo BOOTP possa essere disattivato. Può essere disabilitato usando la funzione Module Configuration nel software RSLinx.

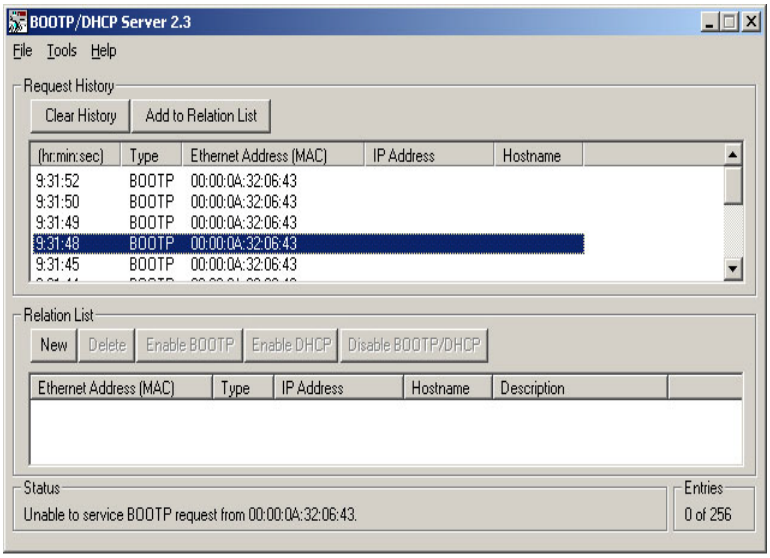
Utilizzo della utility BOOTP di Rockwell

L'utility BOOTP di Rockwell è un programma autonomo che integra la funzionalità di software BOOTP standard con un'interfaccia grafica intuitiva. È possibile scaricarlo all'indirizzo http://www.rockwellautomation.com/rockwellsoftware/download/. Per usare l'utility, il dispositivo deve avere l'abilitazione BOOTP (valore predefinito in fabbrica).

Per configurare il dispositivo usando l'utility BOOTP, procedere come segue.

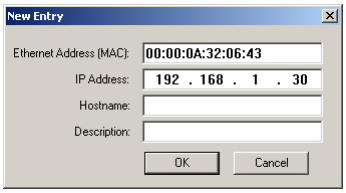
1. Eseguire il software BOOTP.

   Nel riquadro BOOTP Request History vengono visualizzati gli indirizzi hardware dei dispositivi che emettono richieste BOOTP.



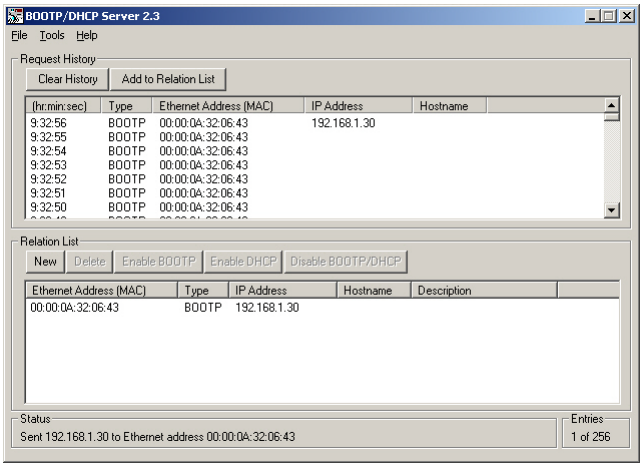
2. Fare doppio clic sull'indirizzo hardware del dispositivo che si desidera configurare.

   Viene visualizzata la finestra contestuale New Entry con l'indirizzo Ethernet (MAC) del dispositivo.



3. Inserire l'indirizzo IP (Hostname e Description sono opzionali) che si desidera assegnare al dispositivo e fare clic su OK.

Il dispositivo sarà aggiunto alla Relation List e verranno visualizzati indirizzo Ethernet (MAC) e indirizzo IP, maschera di sottorete e gateway corrispondenti (se applicabile).

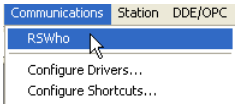


Utilizzo del software RSLinx per impostare l'indirizzo IP

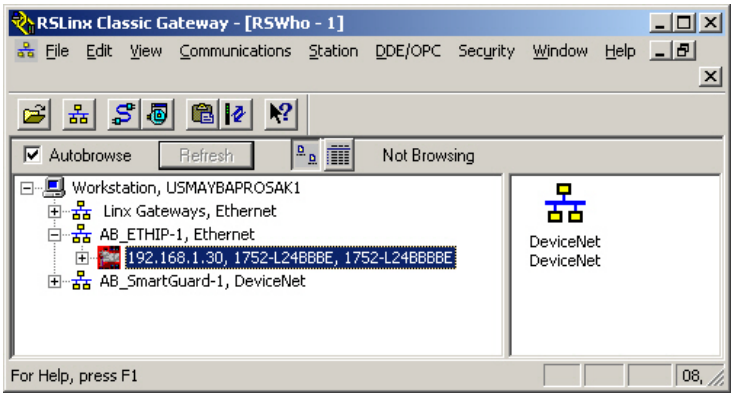
Dopo aver utilizzato l'utility BOOTP per impostare inizialmente l'indirizzo IP di un nuovo controllore SmartGuard 600, è possibile usare il software RSLinx per cambiare l'indirizzo IP. Se questa è la funzionalità che si desidera, verificare di disabilitare l'utility BOOTP nel controllore SmartGuard, altrimenti ogni volta che si applica l'alimentazione, il controllore SmartGuard si accenderà in modalità BOOTP.

Per usare il software RSLinx per configurare i parametri dell'indirizzo IP nel controllore 1752-L24BBBE, procedere come segue.

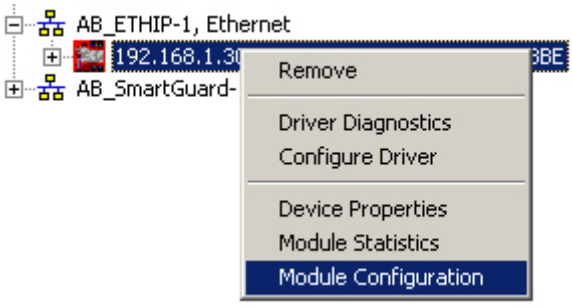
1. Verificare che il controllore 1752-L24BBBE sia installato e acceso.
2. Avviare il software RSLinx.
3. Dal menu a discesa Communications, selezionare RSWho.



Viene visualizzata la finestra di dialogo RSWho.

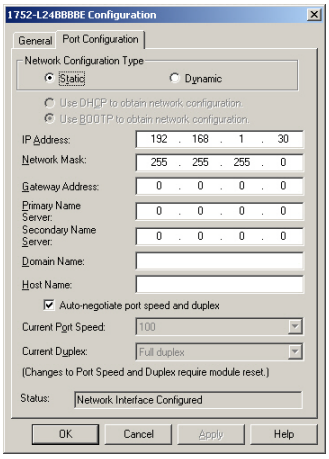


4. Navigare in RSWho fino alla rete Ethernet.
5. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Module Configuration.



SUGGERIMENTO L'opzione di configurazione del modulo compare anche quando si visualizza il controllore SmartGuard dal software DeviceNet ma la configurazione IP viene applicata solo quando viene eseguita direttamente dalla rete EtherNet/IP.

Viene visualizzata la finestra di dialogo Module Configuration.



6. Fare clic sulla scheda Port Configuration.
7. Per Network Configuration Type, fare clic su Static per assegnare permanentemente questa configurazione alla porta.

IMPORTANTE Se si seleziona Dynamic, in caso di spegnimento e riaccensione, il controllore cancella l'attuale configurazione IP e riprende ad inviare richieste BOOTP. Vedere a pagina 55 per ulteriori informazioni.

a. Nel campo IP Address, digitare l'indirizzo IP.
b. Nel campo Network Mask, digitare l'indirizzo della maschera di rete.
c. Nel campo Gateway Address, digitare l'indirizzo del gateway o lasciare a zero.
d. Nel campo Primary Name Server, digitare l'indirizzo del server nomi primario o lasciare a zero.
e. Nel campo Secondary Name Server, digitare l'indirizzo del server nomi secondario o lasciare a zero.
f. Nel campo Domain Name, digitare il nome del dominio o lasciare vuoto.
g. Nel campo Host Name, digitare il nome dell'host o "SmartGuard ENIP".

8. Configurare le impostazioni della porta.

A	Procedere come segue:
Utilizzare le impostazioni di default per la velocità della porta e duplex	Lasciare selezionata la casella di controllo Auto-negotiate port speed and duplex. **IMPORTANTE:** la velocità di default della porta è 100 e l'impostazione duplex di default è Full.
Configurare manualmente le impostazioni relative a velocità della porta e duplex.	a. Deselezionare la casella di controllo Auto-negotiate port speed and duplex. b. Dal menu a discesa Current Port Speed, selezionare una velocità per la porta. c. Dal menu a discesa Current Duplex, selezionare Half Duplex.

9. Fare clic su OK.

Funzione di bridge tra le reti

Il controllore 1752-L24BBBE ha la capacità di collegare in bridge o instradare la comunicazione a vari dispositivi, a seconda delle capacità della piattaforma e dei dispositivi di comunicazione.

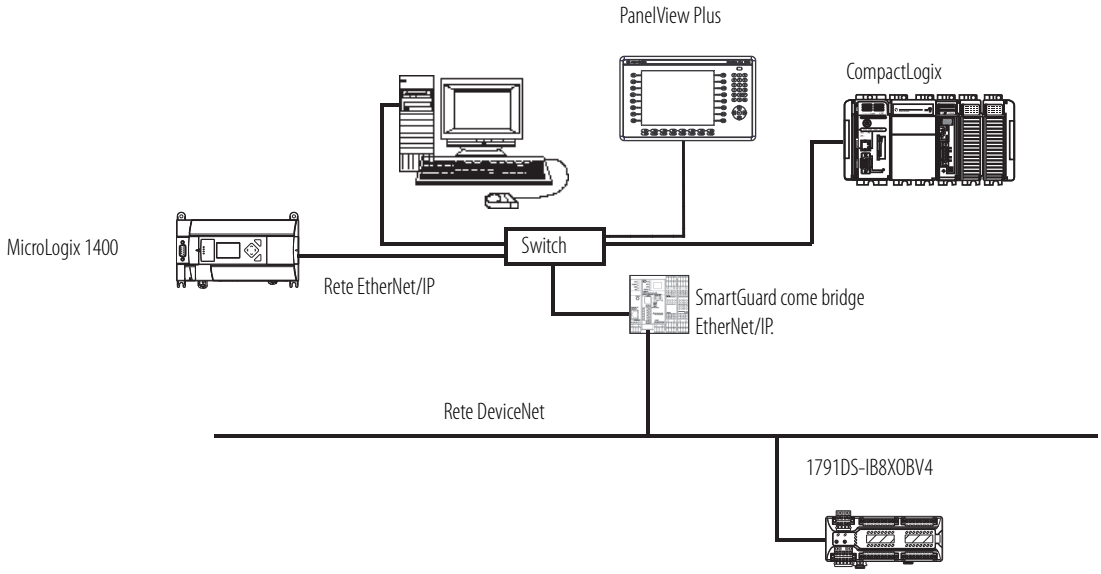
Esiste un bridge quando esiste una connessione tra dispositivi di comunicazione su due reti. Ad esempio, un dispositivo bridge ha connessioni sia EtherNet/IP che DeviceNet, permettendo al Dispositivo 1 su EtherNet/IP di comunicare con il Dispositivo 2 su DeviceNet.

Comunicazione da una rete EtherNet/IP ad una rete DeviceNet

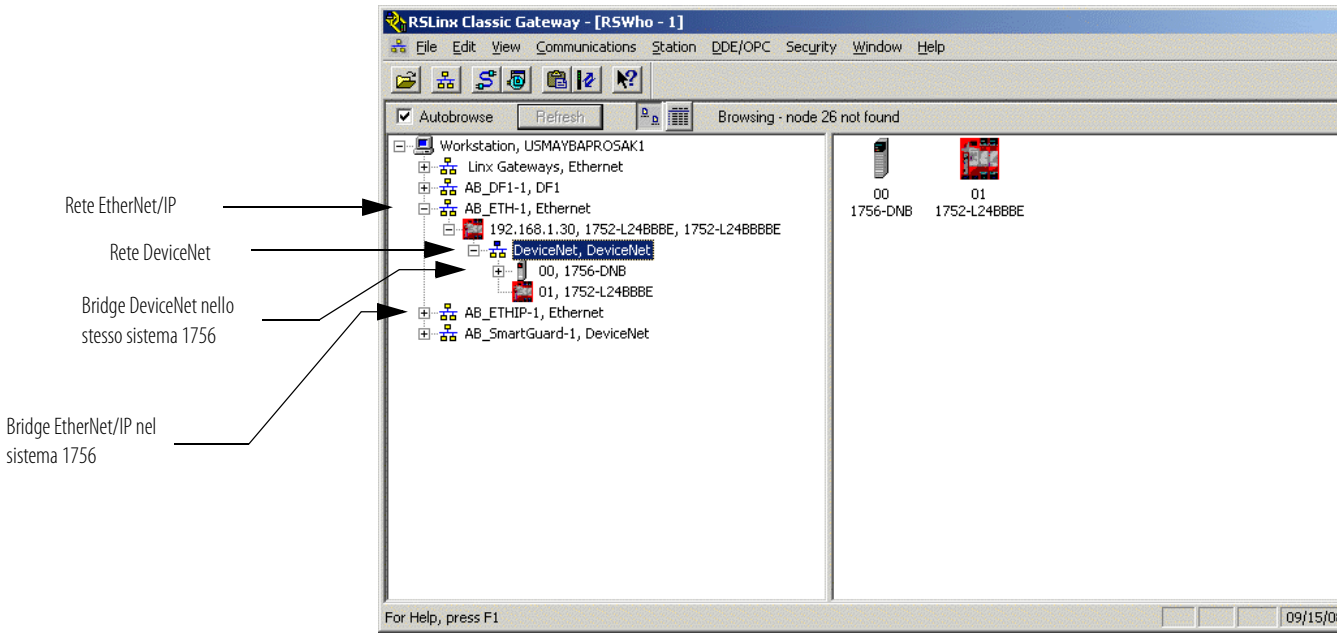
Si tratta di una connessione tra la rete EtherNet/IP e la rete DeviceNet. Il controllore SmartGuard, agendo da bridge, consente di usare un personal computer collegato alla rete EtherNet/IP per configurare il modulo 1791DS sulla rete.

IMPORTANTE La funzione di bridge del controllore SmartGuard è limitata. È concepito per configurare moduli DIO di sicurezza su un'altra rete ma non dovrebbe essere utilizzato per programmare altri PLC e non deve essere usato come dispositivo con funzioni di bridge durante il funzionamento della macchina.

Comunicazione da una rete EtherNet/IP ad una rete DeviceNet



Collegamento in bridge EtherNet/IP ad una rete DeviceNet

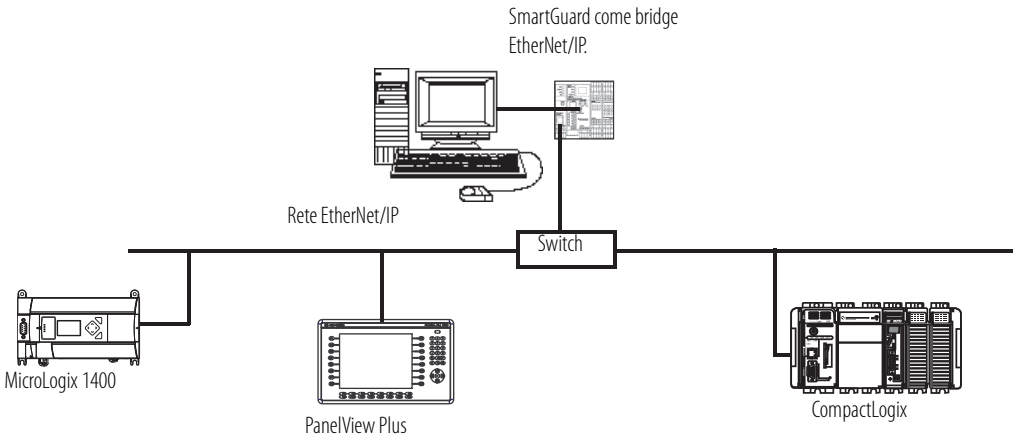


Comunicazione tra la porta USB e rete EtherNet/IP

Il controllore SmartGuard supporta la funzione di bridge dalla porta USB alla rete EtherNet/IP. Tuttavia, per configurare dispositivi diversi dal controllore SmartGuard, è consigliabile non usare questa funzione ma collegarsi direttamente alla rete EtherNet/IP.

Il controllore SmartGuard può esplorare solo la sottorete Ethernet a cui è collegato. È possibile esplorare un controllore MicroLogix 1400 o un controllore CompactLogix ma non un controllore ControlLogix perché è impossibile superare il modulo 1756-ENBT nello chassis ControlLogix.

Comunicazione tra porta USB e rete EtherNet/IP



Gestione del numero della rete di sicurezza (SNN)

Introduzione

Argomento	Pagina
Formati del numero della rete di sicurezza (SNN)	63
Assegnazione del numero della rete di sicurezza (SNN)	65
Impostazione del numero della rete di sicurezza (SNN) in tutti i nodi di sicurezza	66
Numero della rete di sicurezza (SNN) non corrispondente	67
Modifiche del numero della rete di sicurezza (SNN) e dell'indirizzo di nodo	67

Per ogni dispositivo DeviceNet Safety deve essere configurato un numero della rete di sicurezza (SNN). La combinazione del numero SNN e dell'indirizzo di nodo DeviceNet fornisce un identificativo univoco per ogni nodo di sicurezza in una rete industriale complessa che impedisce che i dati destinati ad un indirizzo di nodo specifico su una sottorete DeviceNet vengano instradati erroneamente e accettati da un nodo con lo stesso indirizzo di nodo su una differente sottorete DeviceNet.

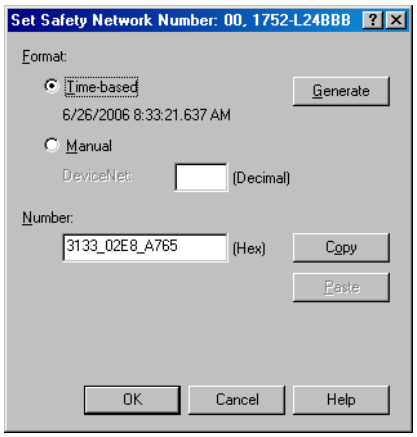
I numeri della rete di sicurezza assegnati a ogni rete di sicurezza o sottorete devono essere univoci. È necessario verificare che venga assegnato un numero della rete di sicurezza (SNN) univoco a ogni rete DeviceNet con nodi di sicurezza.

Formati del numero della rete di sicurezza (SNN)

Il numero della rete di sicurezza (SNN) può essere assegnato dal software (basato sul tempo) o dall'utente (manuale). Nelle sezioni seguenti vengono descritti i due formati del numero SNN.

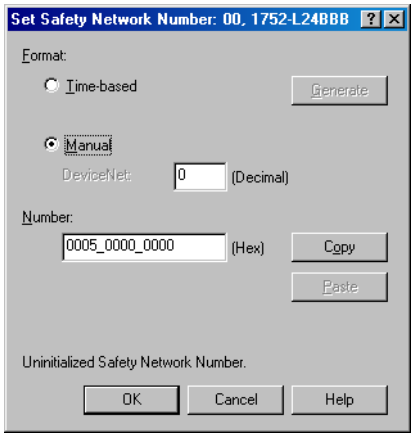
Numero della rete di sicurezza basato sul tempo (consigliato)

Nel formato basato sul tempo, il numero della rete di sicurezza (SNN) rappresenta la data e l'ora di generazione del numero, in base al PC che esegue il software RSNetWorx per DeviceNet.



Numero della rete di sicurezza (SNN) manuale

Nel formato manuale, il numero SNN rappresenta i valori decimali da 1 a 9999 immessi.



SUGGERIMENTO Fare clic su Copy nella finestra di dialogo Set Safety Network Number per copiare il numero SNN negli Appunti di Windows.

Assegnazione del numero della rete di sicurezza (SNN)

È possibile generare automaticamente un numero SNN tramite il software RSNetWorx per DeviceNet oppure assegnarlo manualmente. Un numero SNN generato automaticamente è sufficiente e consigliato per la maggior parte delle applicazioni.

Automatico (basato sul tempo)

Quando un nuovo dispositivo di sicurezza viene aggiunto alla configurazione di rete, un numero SNN di default viene assegnato automaticamente tramite il software di configurazione, come descritto di seguito.

- Se nella configurazione di rete DeviceNet è già presente almeno un dispositivo di sicurezza, ai dispositivi di sicurezza aggiunti successivamente alla configurazione di rete viene assegnato lo stesso numero SNN del dispositivo di sicurezza con indirizzo minore.
- Se nella configurazione di rete DeviceNet non sono presenti altri dispositivi di sicurezza, un numero SNN basato sul tempo viene generato automaticamente dal software RSNetWorx per DeviceNet.

Manuale

L'opzione di assegnazione manuale deve essere utilizzata per i sistemi con un numero limitato di sottoreti DeviceNet e di reti interconnesse in cui si desidera gestire e assegnare i numeri SNN in modo logico in base ad applicazioni specifiche.

IMPORTANTE Se si assegna manualmente un numero SNN, verificare che l'espansione del sistema non produca un duplicato della combinazione di numero SNN e indirizzo di nodo.

Per impostare il numero SNN in un dispositivo di sicurezza tramite il software RSNetWorx per DeviceNet, selezionare il dispositivo nella vista grafica dell'hardware e selezionare Set Safety Network Number dal menu Device.

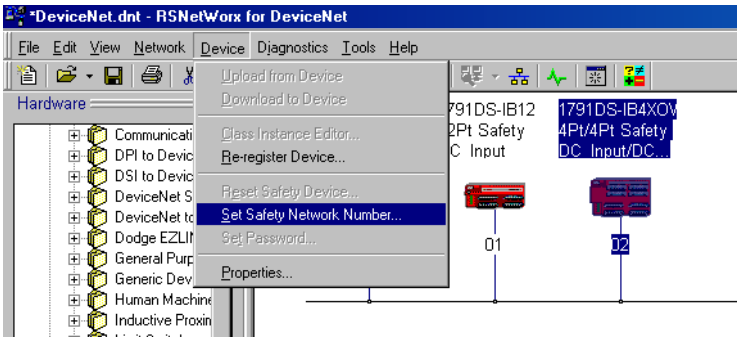
IMPORTANTE Quando viene impostato il numero SNN, viene ripristinata la configurazione di default di fabbrica del dispositivo.

Impostazione del numero della rete di sicurezza (SNN) in tutti i nodi di sicurezza

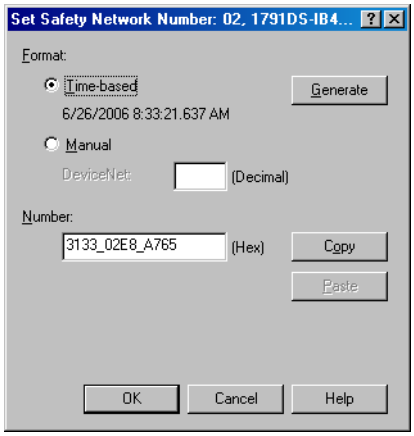
Un numero SNN basato sul tempo viene generato automaticamente quando il primo nuovo dispositivo di sicurezza viene aggiunto alla rete. Ai dispositivi successivamente aggiunti alla rete viene assegnato lo stesso numero SNN del dispositivo di sicurezza con indirizzo minore. Il numero automatico SNN basato sul tempo è sufficiente e consigliato per la maggior parte delle applicazioni.

Attenersi alla procedura seguente per impostare il numero SNN per un dispositivo specifico.

1. Fare clic sul dispositivo di destinazione nella vista grafica dell'hardware, quindi selezionare Set Safety Network Number dal menu Device.



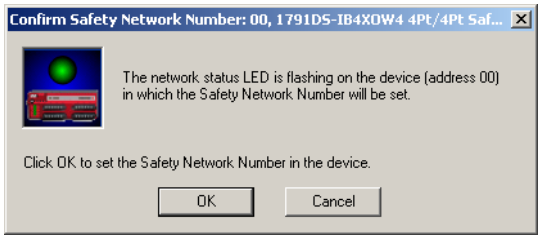
2. Selezionare Time-based e fare clic su Generate oppure selezionare Manual e immettere un numero decimale da 1 a 9999.



3. Fare clic su OK.

SUGGERIMENTO È possibile utilizzare i pulsanti Copy e Paste nella finestra di dialogo Set Safety Network Number per copiare e incollare un numero SNN tra i dispositivi e per annotare il numero SNN.

4. Verificare che l'indicatore dello stato di rete lampeggi rapidamente in rosso e in verde, alternativamente, sul dispositivo corretto, quindi fare clic su OK.

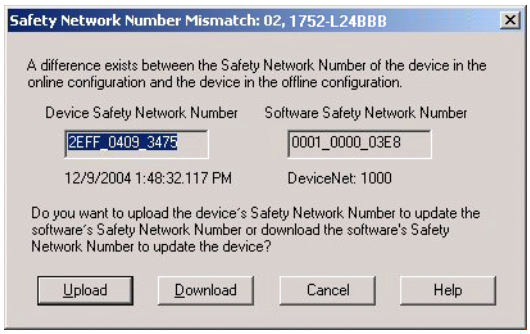


Numero della rete di sicurezza (SNN) non corrispondente

Il software RSNetWorx per DeviceNet confronta il numero SNN offline e il numero SNN online durante ogni operazione di esplorazione, one-shot o continua, e durante le operazioni di caricamento o download. Se i numeri SNN non corrispondono, il software RSNetWorx per DeviceNet segnala un errore di SNN. Nella vista grafica dell'hardware viene visualizzato il simbolo ! sull'icona del dispositivo di sicurezza.

In modalità Online, il software RSNetWorx for DeviceNet verifica anche la corrispondenza SNN quando viene selezionata la finestra di dialogo Device Properties di un dispositivo di sicurezza, sia dal menu Device > Properties sia facendo doppio clic sul dispositivo. Se i numeri SNN non corrispondono, viene visualizzata la finestra di dialogo Safety Network Number Mismatch.

Nella finestra di dialogo Safety Network Number Mismatch vengono visualizzati il numero SNN online (dispositivo) e il numero SNN offline (software). Per risolvere il problema, è possibile scegliere di caricare il numero SNN del dispositivo o di scaricare il numero SNN offline.



Se il numero SNN del dispositivo non è stato inizializzato, nel campo Device Safety Network Number viene riportato il numero SNN di default: FFFF_FFFF_FFFF. Quando il numero SNN del dispositivo è FFFF_FFFF_FFFF, il pulsante Upload risulta inattivo (grigio) e non è disponibile.

Modifiche del numero della rete di sicurezza (SNN) e dell'indirizzo di nodo

Per modificare l'indirizzo di un dispositivo di sicurezza, è necessario prima annullare l'inizializzazione del numero SNN oppure ripristinarlo.

Attenersi alla procedura seguente per ripristinare il numero SNN.

1. Selezionare il dispositivo nella vista grafica dell'hardware.
2. Dal menu Device, selezionare Reset Safety Device.
3. Selezionare la casella di controllo Safety Network Number nella finestra di dialogo Reset Safety Device e fare clic su Reset.

   Vengono ripristinate le impostazioni di default di fabbrica solo per gli attributi selezionati nella finestra di dialogo. Il ripristino di sicurezza ha effetto solo sul dispositivo di sicurezza; la configurazione del progetto RSNetWorx non viene persa.

Per ulteriori informazioni sulla funzione di ripristino di sicurezza, vedere Ripristino di sicurezza (opzionale) a pagina pagina 46.

SUGGERIMENTO

Dopo il ripristino di sicurezza, è possibile modificare l'indirizzo di nodo nel software RSNetWorx per DeviceNet facendo doppio clic sull'indirizzo di nodo del dispositivo di sicurezza nella vista grafica. Una volta modificato l'indirizzo di nodo, fare clic con il pulsante destro del mouse sul dispositivo, quindi fare clic su Download to Device per ripristinare il numero SNN e la configurazione del dispositivo di sicurezza.

Configurazione dell'I/O locale

Introduzione

Argomento	Pagina
Configurazione degli ingressi di sicurezza locali	69
Configurazione delle uscite di test locali	74
Configurazione delle uscite di sicurezza locali	76

Configurazione degli ingressi di sicurezza locali

Il controllore è dotato di 16 ingressi di sicurezza locali che supportano le seguenti funzionalità.

- Diagnosi del circuito di ingresso – È possibile utilizzare sorgenti di test a impulsi per monitorare i circuiti interni, i dispositivi esterni e il cablaggio esterno.
- Ritardi all'eccitazione e alla diseccitazione dell'ingresso: è possibile impostare dei filtri per il tempo di ingresso, compresi tra 0 e 126 ms in multipli della durata del ciclo del controllore. L'impostazione di ritardi all'eccitazione e alla diseccitazione dell'ingresso consente di ridurre l'influenza di chattering (oscillazioni) e dei disturbi esterni.

IMPORTANTE I ritardi all'eccitazione o alla diseccitazione devono essere aggiunti al tempo di risposta I/O. Questo influirà sui calcoli dei tempi di reazione del sistema.

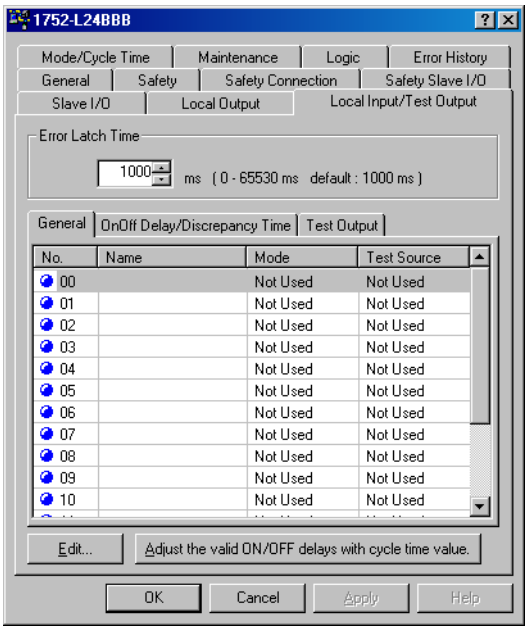
Per informazioni sul calcolo dei tempi di reazione, consultare il manuale di riferimento per la sicurezza "Controllori SmartGuard 600", pubblicazione 1752-RM001B-IT-P.

- Modalità Doppio canale – È possibile impostare la modalità Doppio canale per coppie di ingressi locali associate. Se è stata impostata la modalità Canale duale, è possibile valutare le discrepanze temporali nelle modifiche di dati o nei segnali di ingresso tra due ingressi locali accoppiati.

Attenersi alla seguente procedura per configurare gli ingressi di sicurezza locali.

1. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Properties.

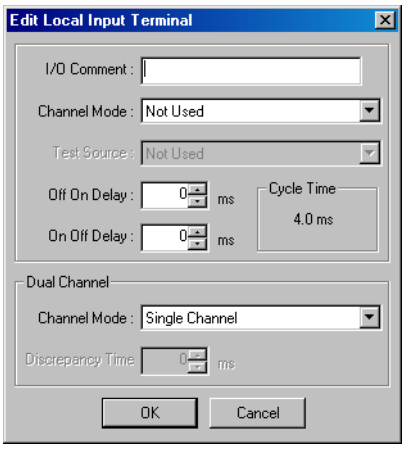
2. Selezionare la scheda Local Input/Test Output.



3. Impostare il tempo di mantenimento dello stato di errore.

   Il tempo di mantenimento dello stato di errore è valido per tutti gli ingressi di sicurezza e le uscite di test e consente di impostare il tempo per cui mantenere lo stato di errore quando si verifica un errore in un ingresso o in una uscita. Anche se l'errore viene eliminato, lo stato di errore viene sempre mantenuto per il tempo di mantenimento dello stato di errore configurato. Il tempo di mantenimento dello stato di errore può essere impostato su un valore compreso tra 0 e 65530 ms in incrementi di 10 ms. L'impostazione di default è 1000 ms.

4. Selezionare un morsetto di ingresso di sicurezza e fare clic su Edit.



5. Immettere un commento I/O.

   Il commento I/O specificato in questa fase viene utilizzato come nome di tag I/O in Logic Editor.

6. Impostare la modalità di canale per l'ingresso di sicurezza.

Modalità canale	Descrizione
Not used	Il canale di ingresso non è collegato a un dispositivo esterno. Si tratta dell'impostazione di default.
Test pulse from test output	Utilizzare questa modalità per i circuiti di ingresso Categoria 4. Si presume che, in questa modalità, il dispositivo di ingresso sia collegato a una sorgente di test a impulsi, quindi cablato al morsetto di ingresso affinché venga abilitato il rilevamento di cortocircuiti sulla linea di alimentazione (polo positivo), di guasti verso terra e di cortocircuiti su altre linee dei segnali di ingresso (corti canale-canale). Il controllore deve essere in grado di rilevare che il segnale di ingresso viene testato con impulsi, altrimenti potrebbero verificarsi interruzioni involontarie. Vedere Esempio: canale di ingresso impostato su Test Pulse from Test Output a pagina 73.
Used as a safety input	Utilizzare questa modalità per collegarsi a un dispositivo di sicurezza con un'uscita a semiconduttori, quale una barriera fotoelettrica.
Used as a standard input	Utilizzare questa modalità per collegarsi a un dispositivo standard (non di sicurezza).

7. Se la modalità di canale viene impostata su Test pulse from test output, scegliere dall'elenco a discesa Test Source l'uscita di test da utilizzare insieme all'ingresso di sicurezza.

SUGGERIMENTO La modalità di canale dell'uscita di test selezionata viene impostata automaticamente su Pulse Test Output.

8. Impostare la modalità Canale duale e il tempo di discrepanza.

L'impostazione della modalità Canale duale consente di valutare e riflettere nei tag I/O lo stato di due ingressi. È inoltre possibile valutare il tempo di discrepanza tra i cambiamenti di stato dei due ingressi. Le combinazioni che possono essere impostate sono predefinite. Il tempo di discrepanza può essere impostato su un valore compreso tra 0 e 65530 ms in incrementi di 10 ms. Entrambi gli ingressi devono cambiare stato entro il tempo di discrepanza, altrimenti si verifica un errore.

Modalità canale	Descrizione
Canale singolo	Il morsetto di ingresso di sicurezza viene utilizzato in modo indipendente.
Doppio canale equivalente	Il morsetto di ingresso di sicurezza viene utilizzato come canale doppio equivalente con un morsetto di ingresso di sicurezza accoppiato.
Doppio canale complementare	Il morsetto di ingresso di sicurezza viene utilizzato come canale doppio complementare con un morsetto di ingresso di sicurezza accoppiato.

SUGGERIMENTO Il controllore supporta i blocchi funzione con una funzionalità equivalente alla modalità Canale duale. In diversi casi, la segnalazione e la ricerca degli errori del sistema è più facile quando per rilevare gli errori si utilizzano i blocchi funzione anziché l'hardware SmartGuard. Se si desidera usare i blocchi funzione per rilevare gli errori del sistema, gli ingressi di sicurezza devono essere configurati per canale singolo.

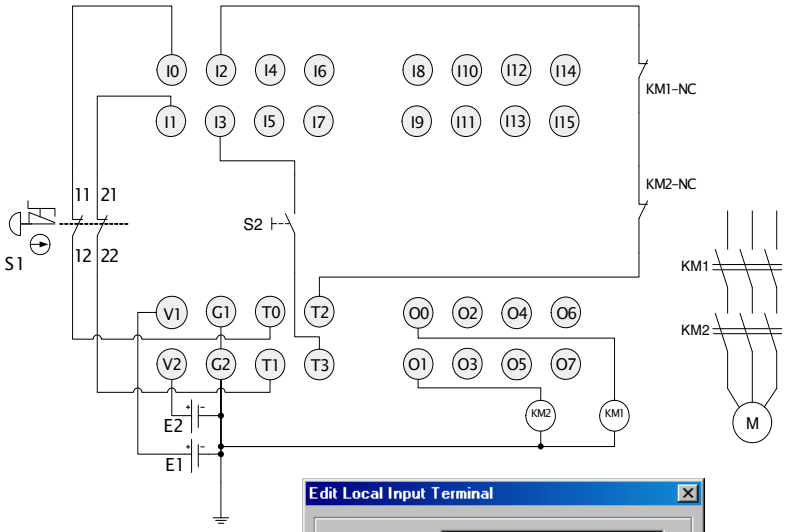
9. Specificare il tempo di ritardo all'eccitazione e alla diseccitazione.

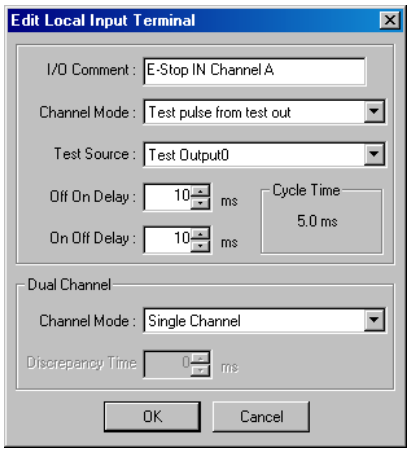
L'intervallo valido è compreso tra 0 e 126 ms, ma il tempo di ritardo deve essere un multiplo della durata del ciclo.

IMPORTANTE Il valore ottimale per la durata del ciclo del controllore viene calcolato automaticamente in base alle impostazioni dei parametri e ai programmi applicativi. Pertanto, impostare per ultimo il tempo di ritardo all'eccitazione e alla diseccitazione.

Esempio: canale di ingresso impostato su Test Pulse from Test Output

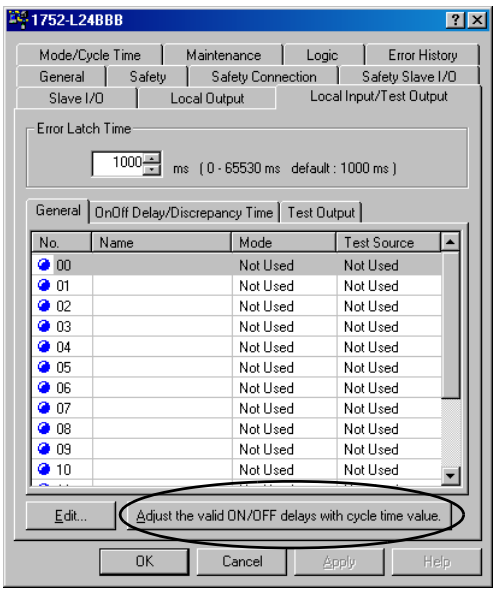
Per il seguente schema di cablaggio, la modalità di canale deve essere impostata su Test pulse from test out, come illustrato.





Regolazione automatica del tempo di ritardo all'eccitazione e alla diseccitazione

Se i parametri relativi alla durata del ciclo vengono modificati dopo l'impostazione dei ritardi all'eccitazione e alla diseccitazione, potrebbe non essere possibile chiudere la finestra di dialogo Controller Properties a causa di un errore nell'impostazione dei parametri. In questo caso, è possibile riconfigurare i tempi di ritardo all'eccitazione e alla diseccitazione in base alla durata del ciclo utilizzando il pulsante Adjust valid ON/OFF delays with cycle time value nella scheda Local Input/Test Output.



Configurazione delle uscite di test locali

Le quattro uscite di test indipendenti possono essere utilizzate insieme agli ingressi di sicurezza. Inoltre, possono essere impostate per essere utilizzate come morsetti di uscita standard. Di seguito sono elencate le funzionalità delle uscite a impulsi di test.

- Rilevamento della corrente per la spia di muting: è possibile rilevare scollegamenti o guasti della lampadina solo per il morsetto T3.
- Rilevamento e protezione da sovracorrente – Per proteggere il circuito elettrico, l'uscita viene bloccata in caso di rilevamento di sovracorrente.

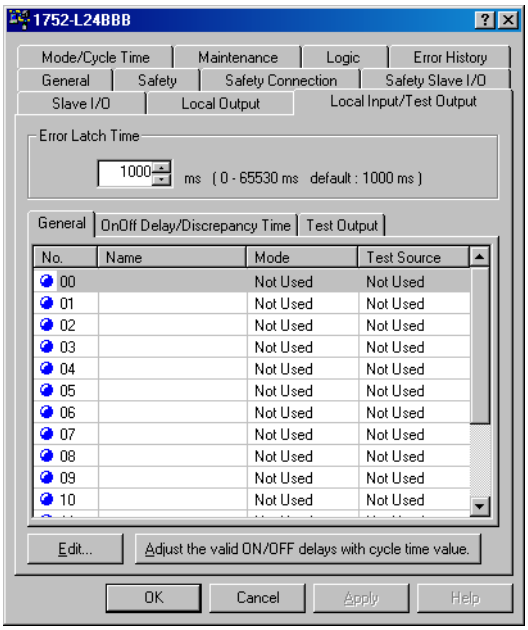
ATTENZIONE

Le uscite a impulsi non devono essere utilizzate come uscite di sicurezza (ad esempio, per il controllo di attuatori di sicurezza) poiché non sono classificate come sicure.

Attenersi alla seguente procedura per configurare un'uscita di test.

1. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Properties.

2. Selezionare la scheda Local Input/Test Output.

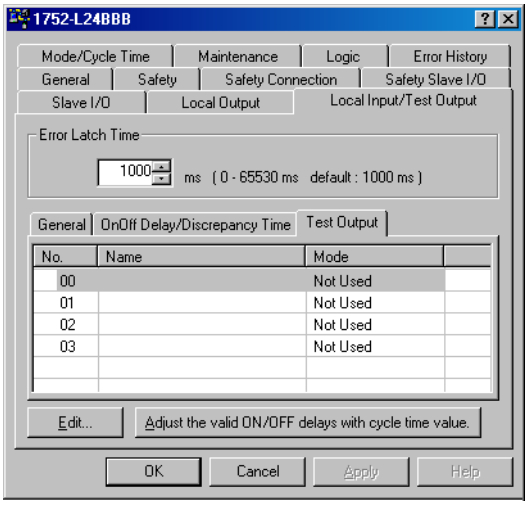


3. Impostare il tempo di mantenimento dello stato di errore.

   Il tempo di mantenimento dello stato di errore è valido per tutti gli ingressi di sicurezza e le uscite di test e consente di impostare il tempo per cui mantenere lo stato di errore quando si verifica un errore in un ingresso o in una uscita. Anche se l'errore viene eliminato, lo stato di errore viene sempre mantenuto per il tempo di mantenimento dello stato di errore configurato. Il tempo di mantenimento dello stato di errore può essere impostato su un valore compreso tra 0 e 65530 ms in incrementi di 10 ms. L'impostazione di default è 1000 ms.

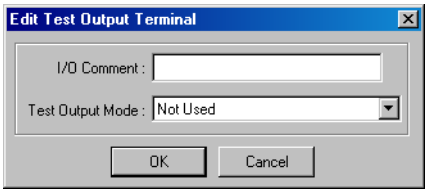
4. Selezionare la scheda Test Output.

5. Selezionare un morsetto di uscita di test e fare clic su Edit.



6. Immettere un commento I/O.

   Il commento I/O specificato in questa fase viene utilizzato come nome di tag I/O in Logic Editor.



7. Selezionare una modalità di uscita di test dall'elenco a discesa Test Output Mode.

Modalità di uscita di test	Descrizione
Not used	L'uscita di test corrispondente non viene utilizzata.
Standard Output	Scegliere questa modalità quando si effettua il collegamento all'uscita da una spia di muting o da un controllore a logica programmabile. L'uscita viene utilizzata come uscita di controllo.
Pulse Test Output	Scegliere questa modalità quando si collega un dispositivo a un'uscita a contatti insieme a un ingresso di sicurezza.
Muting Lamp Output	Scegliere questa modalità per specificare un'uscita spia di muting. Questa impostazione è supportata solo sul morsetto T3. Quando l'uscita è attivata, è possibile rilevare lo scollegamento della spia di muting.

Configurazione delle uscite di sicurezza locali

Il controllore è dotato di otto uscite di sicurezza locali che supportano le funzioni elencate di seguito.

- Diagnosi del circuito di uscita – È possibile utilizzare impulsi di test per monitorare i circuiti interni, i dispositivi esterni e il cablaggio esterno del controllore.
- Rilevamento e protezione da sovracorrente – Per proteggere il circuito elettrico, l'uscita viene bloccata in caso di rilevamento di sovracorrente.
- Modalità Canale duale – È possibile impostare lo stato di sicurezza per entrambe le uscite accoppiate in caso di errore in una delle uscite locali accoppiate, indipendentemente dal programma utente.

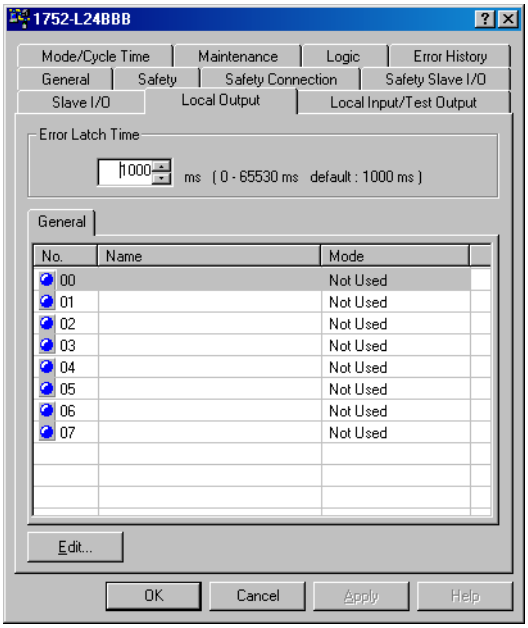
Attenersi alla seguente procedura per configurare un'uscita di sicurezza locale.

1. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Properties.

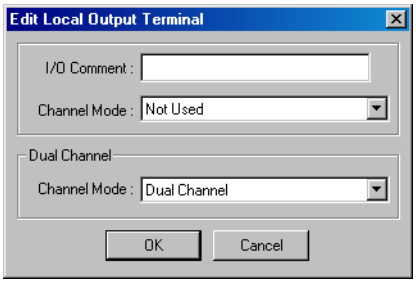
2. Selezionare la scheda Local Output.

3. Impostare il tempo di mantenimento dello stato di errore.

   Il tempo di mantenimento dello stato di errore è valido per tutte le uscite di sicurezza e consente di impostare il tempo per cui mantenere lo stato di errore quando si verifica un errore in un ingresso o in una uscita. Anche se l'errore viene eliminato, lo stato di errore viene sempre mantenuto per il tempo di mantenimento dello stato di errore configurato. Il tempo di mantenimento dello stato di errore può essere impostato su un valore compreso tra 0 e 65530 ms in incrementi di 10 ms. Il valore di default è 1000 ms.



4. Selezionare un morsetto di uscita di sicurezza e fare clic su Edit.



5. Immettere un commento I/O.

   Il commento I/O specificato in questa fase viene utilizzato come nome di tag I/O in Logic Editor.

6. Impostare la modalità di canale per l'uscita di sicurezza.

Modalità canale	Descrizione
Not used	Il morsetto di uscita non è collegato a un dispositivo di uscita.
Sicurezza	Non viene inviato un impulso di test quando l'uscita è attivata. Quando l'uscita è disattivata, è possibile rilevare cortocircuiti sulla linea di alimentazione. Inoltre, è possibile rilevare guasti verso terra.
Test a impulsi di sicurezza	Viene inviato un impulso di test quando l'uscita è attivata. In questo modo viene abilitato il rilevamento dei cortocircuiti sulla linea di alimentazione (polo positivo) sia con l'uscita attivata che disattivata. Inoltre, è possibile rilevare guasti verso terra e cortocircuiti tra segnali di uscita.

IMPORTANTE Se è impostato un test a impulsi di sicurezza, all'attivazione dell'uscita di sicurezza viene generato un segnale di impulsi di disattivazione (ampiezza di impulso 580 µs) per effettuare una diagnosi del circuito di uscita. Al fine di accertarsi che l'impulso di uscita non causi malfunzionamenti, verificare il tempo di risposta dell'ingresso del dispositivo di controllo.

7. Impostare la modalità Canale duale per l'uscita di sicurezza.

L'impostazione della modalità Canale duale consente il rilevamento di un errore se le due uscite di un programma utente non sono equivalenti. Se viene rilevato un errore in uno dei due circuiti delle uscite, verranno disattivate entrambe le uscite del dispositivo.

Impostazioni della modalità Doppio canale dell'uscita

Modalità canale	Descrizione
Canale singolo	Il morsetto di uscita di sicurezza viene utilizzato in modo indipendente.
Doppio canale	Il morsetto di uscita di sicurezza è accoppiato con un altro morsetto di uscita. È possibile attivare l'uscita quando sia l'uscita che l'uscita di sicurezza abbinata corrispondono.

Configurazione del controllore per le comunicazioni DeviceNet

Introduzione

Il controllore SmartGuard può funzionare contemporaneamente come master di sicurezza, slave di sicurezza o slave standard.

Argomento	Pagina
Configurazione del controllore come master di sicurezza	79
Configurazione del controllore come slave di sicurezza	90
Configurazione del controllore come slave DeviceNet standard	98
Lettura e scrittura tra il controllore SmartGuard e un'interfaccia PanelView Plus	103

Configurazione del controllore come master di sicurezza

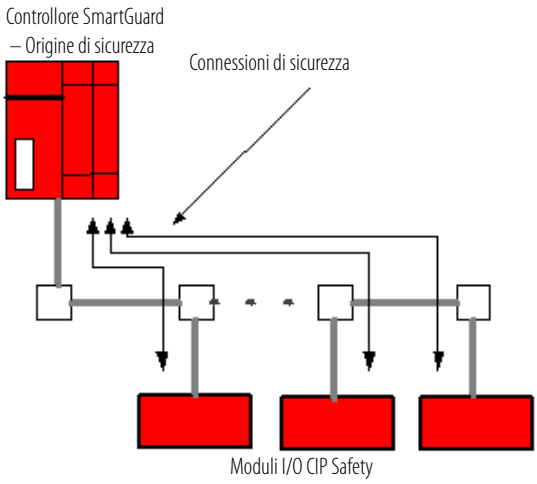
Come master di sicurezza, il controllore può eseguire comunicazioni I/O di sicurezza con un massimo di 32 collegamenti, utilizzando fino a 16 byte per collegamento. I collegamenti possono essere uni-cast o multi-cast.

Sono disponibili 32 collegamenti e ogni differente tipo di modulo I/O distribuito di sicurezza ne utilizza un numero diverso. Ad esempio, un modulo di solo ingresso può utilizzare 1 dei 32 collegamenti (collegamento di ingresso), mentre un modulo con ingressi e uscite può utilizzare 2 dei 32 collegamenti di sicurezza (1 collegamento di ingresso e 1 collegamento di uscita).

Il numero di collegamenti di sicurezza utilizzati viene determinato anche dalla configurazione del modulo. Ad esempio, il modulo 1791DS-IB12 è dotato di 12 ingressi di sicurezza, nessuna uscita di sicurezza e 4 uscite di test a impulsi o standard. Se il modulo viene configurato solo per gli ingressi di sicurezza, utilizza 1 collegamento di sicurezza. Tuttavia, se viene configurato per l'utilizzo di ingressi di sicurezza e uscite standard, il modulo utilizza 2 collegamenti di sicurezza. Infine, il numero e il tipo di modulo I/O distribuito di sicurezza collegato al controllore SmartGuard determina il numero massimo di moduli gestibili dal controllore.

Per ogni collegamento sulla rete di sicurezza DeviceNet viene stabilita una relazione master-slave, separata dalle comunicazioni master-slave sulla rete standard DeviceNet. In questo modo, il controllore master di sicurezza viene abilitato al controllo dei collegamenti di sicurezza.

Controllore SmartGuard come master di sicurezza

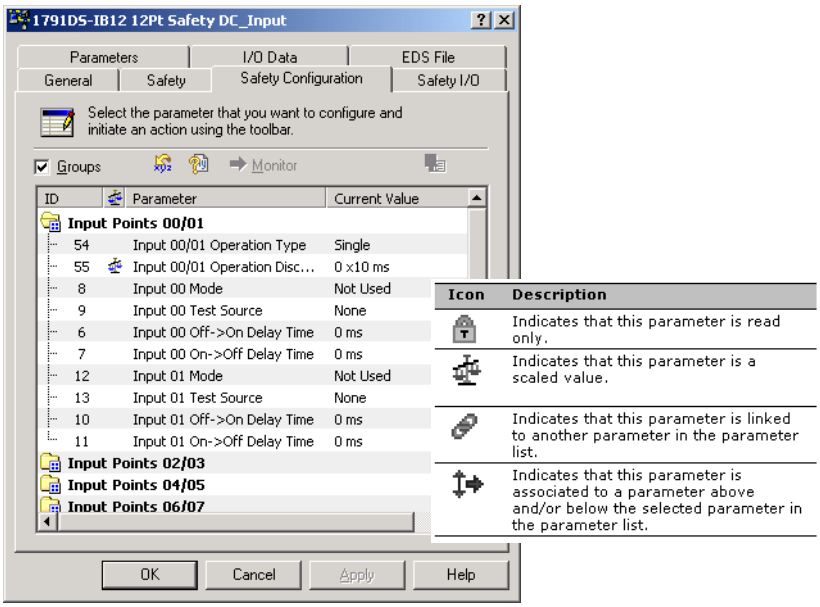


Configurazione delle destinazioni I/O CIP Safety sulla rete DeviceNet

Per configurare il modulo, fare doppio clic sul modulo nella visualizzazione grafica oppure fare clic con il pulsante destro del mouse sul modulo e selezionare Properties.

Parametri per ingressi, uscite e test di sicurezza

È possibile configurare i parametri di sicurezza utilizzando la scheda Safety Configuration della finestra di dialogo Module Properties.



Confronto tra canale singolo e doppio canale equivalente o complementare

È possibile configurare gli ingressi dei moduli I/O distribuiti per la modalità a canale singolo o doppio. Indica al modulo Guard I/O se considerare gli ingressi individualmente (canale singolo) o come coppie di ingressi (doppio canale). Gli ingressi a doppio canale possono essere configurati come equivalenti – quando entrambi gli ingressi devono essere sempre nello stesso stato – o come complementari, quando entrambi gli ingressi devono essere sempre in stati opposti.

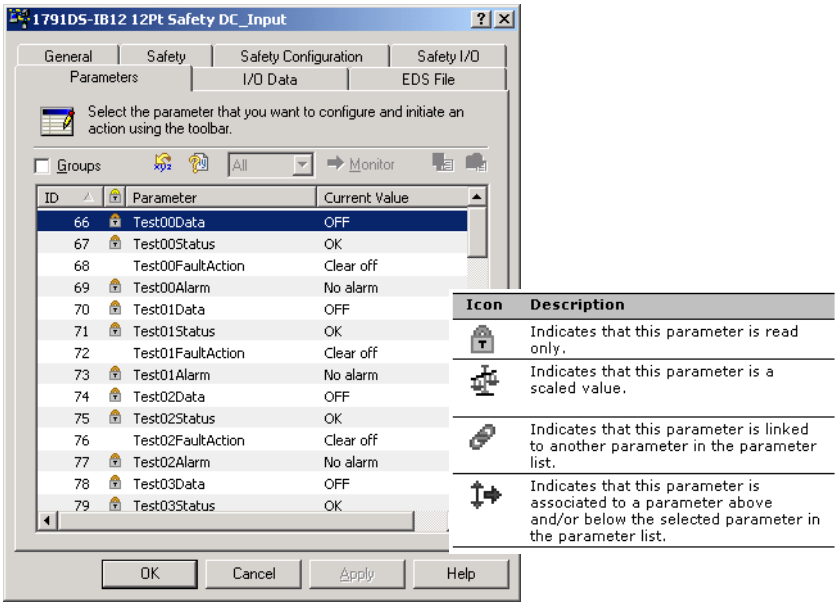
Se configurato in modalità a doppio canale, gli stati di entrambi i canali inviati dal modulo Guard I/O al controllore SmartGuard saranno sempre bassi o alti. Ciò significa che l'errore di incoerenza degli ingressi sull'istruzione SmartGuard non si verificherà mai.

Se si desidera che l'istruzione SmartGuard esegua la diagnostica dell'ingresso di sicurezza sui moduli Guard I/O, configurare i moduli Guard I/O in modalità a canale singolo. Ciò permetterà di usare gli indicatori di errore forniti dalle istruzioni SmartGuard nel programma, scelta decisamente consigliabile.

Se si desidera eseguire la diagnostica dell'ingresso di sicurezza sul modulo Guard I/O con gli indicatori di stato ed i bit di stato del modulo, senza usare la diagnostica delle istruzioni SmartGuard, configurare il modulo Guard I/O in modalità a doppio canale complementare o equivalente.

Parametri degli ingressi e delle uscite standard

I moduli 1791DS descritti in questo manuale supportano dati standard e anche dati di sicurezza. Configurare i parametri degli ingressi e delle uscite standard utilizzando la scheda Parameters della finestra di dialogo Module Properties.



SUGGERIMENTO È possibile che altri dispositivi presentino opzioni di configurazione differenti. Per ulteriori informazioni, consultare il Manuale dell'utente del dispositivo.

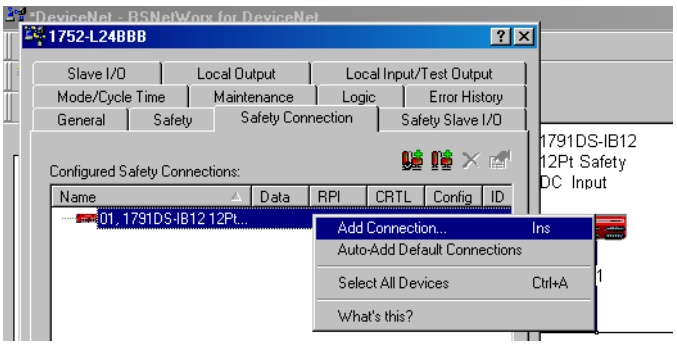
Download delle configurazioni del dispositivo

Una volta configurati i parametri dei moduli I/O standard e di sicurezza, scaricare la configurazione nei moduli. Per farlo, nel software RSNetWorx for DeviceNet, dal menu Device, selezionare Download to Device.

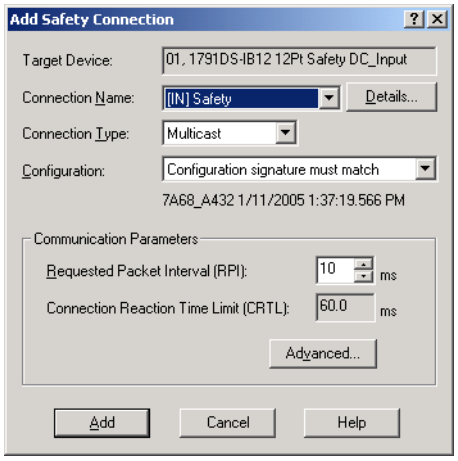
Configurazione dei collegamenti I/O di sicurezza

I collegamenti I/O di sicurezza sono utilizzati per lo scambio automatico dei dati con gli slave di sicurezza senza un programma utente. Per eseguire le comunicazioni I/O di sicurezza con altri slave, è necessario configurare il collegamento con il controllore SmartGuard.

1. Nella scheda Safety Connections, fare clic con il pulsante destro del mouse sul modulo I/O, quindi selezionare Add Connections per visualizzare tutti i collegamenti disponibili.



   La finestra di dialogo Add Safety Connection consente di configurare un collegamento.



2. Selezionare il collegamento desiderato scegliendo il nome collegamento.

3. Selezionare un tipo di collegamento, Multicast (solo per i collegamenti di ingresso) o Point-to-point (collegamenti di ingresso e di uscita).

4. Fare clic sull'opzione Configuration signature must match.

   Questa selezione farà sì che, quando si collega al modulo I/O, il controllore SmartGuard includa l'autenticazione di configurazione e che il modulo I/O accetti la connessione solo se l'autenticazione corrisponde a quella nel dispositivo.

IMPORTANTE Se non viene selezionata l'opzione Configuration signature must match, l'utente deve verificare l'integrità della sicurezza del sistema utilizzando altri strumenti.

5. Verificare l'opzione Connection Reaction Time Limit.

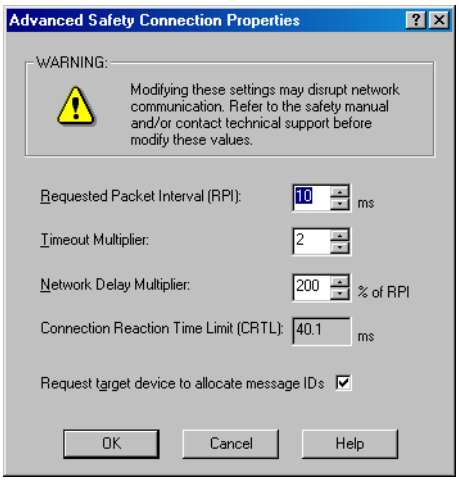
   L'opzione Connection Reaction Time Limit indica la durata massima dei pacchetti di sicurezza sul collegamento associato. Se la durata dei dati utilizzati dal dispositivo consumatore è superiore al limite di tempo di reazione del collegamento, si verifica un errore di collegamento. Configurare il limite di tempo di reazione del collegamento modificando il valore RPI o utilizzando la finestra di dialogo Advanced Communication Properties come descritto ai punti 6 e 7.

6. Impostazione dell'intervallo RPI.

   L'intervallo RPI specifica la frequenza con cui i dati vengono aggiornati durante un collegamento. L'intervallo RPI viene specificato in incrementi di 1 millisecondo ed il controllore supporta un intervallo compreso tra 5 e 500 ms con un'impostazione di default di 10 ms. Altri dispositivi di destinazione potrebbero avere altri vincoli di intervallo RPI limitato. Per determinare l'intervallo supportato e i valori incrementali di ogni tipo di dispositivo di destinazione, consultare la relativa documentazione.

   La modifica dell'intervallo RPI interessa il valore impostato per l'opzione Connection Reaction Time Limit. Per semplici vincoli temporali, in genere è sufficiente impostare l'intervallo RPI. Tuttavia, per requisiti più complessi, fare clic su Advanced per configurare ulteriormente i valori temporali che interessano il tempo di reazione del collegamento.

7. Impostazione della finestra di dialogo Advanced Safety Connection Properties (se richiesto).



- Timeout Multiplier – Il parametro Timeout Multiplier determina il numero di intervalli RPI di attesa di un pacchetto prima di dichiarare il timeout del collegamento, vale a dire il numero di messaggi che possono andare persi prima che venga dichiarato un errore di collegamento. Ad esempio, un Timeout Multiplier pari a 1 indica che i messaggi devono essere ricevuti entro ciascun intervallo RPI. Un Timeout Multiplier pari a 2 indica che 1 messaggio può andare perso se almeno 1 messaggio viene ricevuto in 2 intervalli RPI (2 x RPI).
- Network Delay Multiplier – Il parametro Network Delay Multiplier definisce il tempo di trasporto del messaggio applicato dal protocollo di comunicazione. Questo parametro specifica il ritardo del percorso produttore-consumatore-produttore compiuto dai dati. Il parametro Network Delay Multiplier può essere utilizzato per ridurre o aumentare il valore Connection Reaction Time Limit nei casi in cui il tempo di trasporto del messaggio applicato è notevolmente inferiore o superiore all'intervallo RPI.

8. Dal menu File, selezionare Save per salvare la configurazione.

Modifica di una connessione I/O

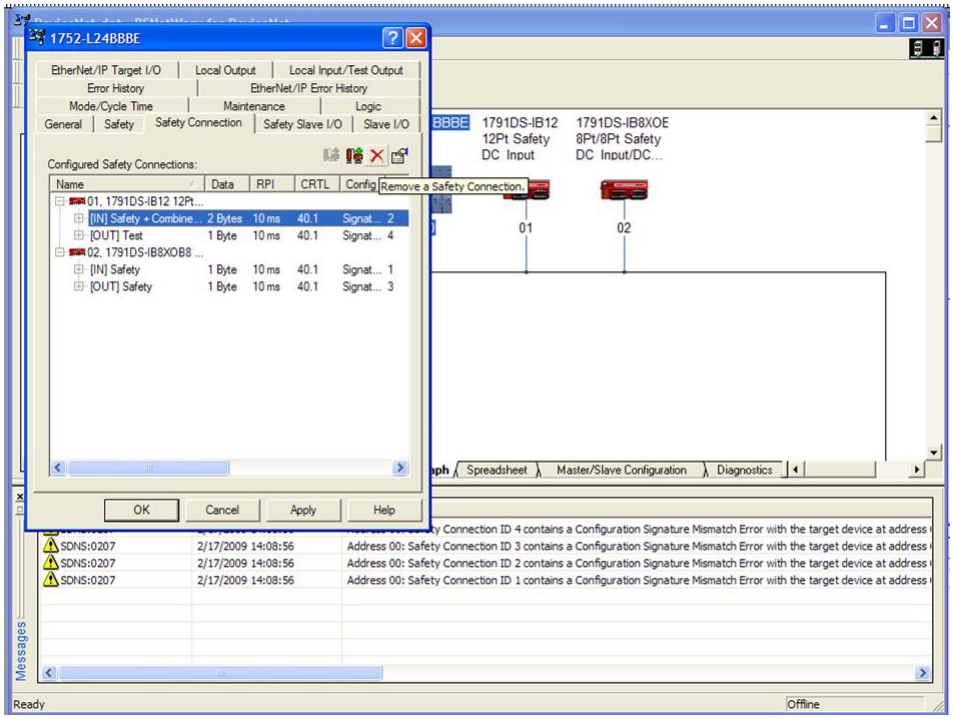
ATTENZIONE

Quando la logica è programmata usando moduli I/O distribuiti (DIO) con il controllore SmartGuard e si elimina (o si elimina e si riaggiunge) una connessione di sicurezza ad un modulo DIO, le connessioni degli I/O remoti nell'editor della logica saranno contrassegnate come non valide e potrebbero essere collegate al blocco funzione sbagliato. Fino a quando questi errori non vengono corretti, sarà impossibile scaricare il programma.

Se si cancella una connessione ad un modulo DIO con logica già scritta, è necessario tornare alla logica e verificare o modificare i tag nel programma in modo che corrispondano ai corretti blocchi funzione. Prima di cancellare o ripristinare le connessioni, prendere nota delle connessioni di sicurezza e delle mappature. Prima di eseguire la logica nell'applicazione, verificare queste connessioni.

Per modificare le connessioni di sicurezza, procedere come segue.

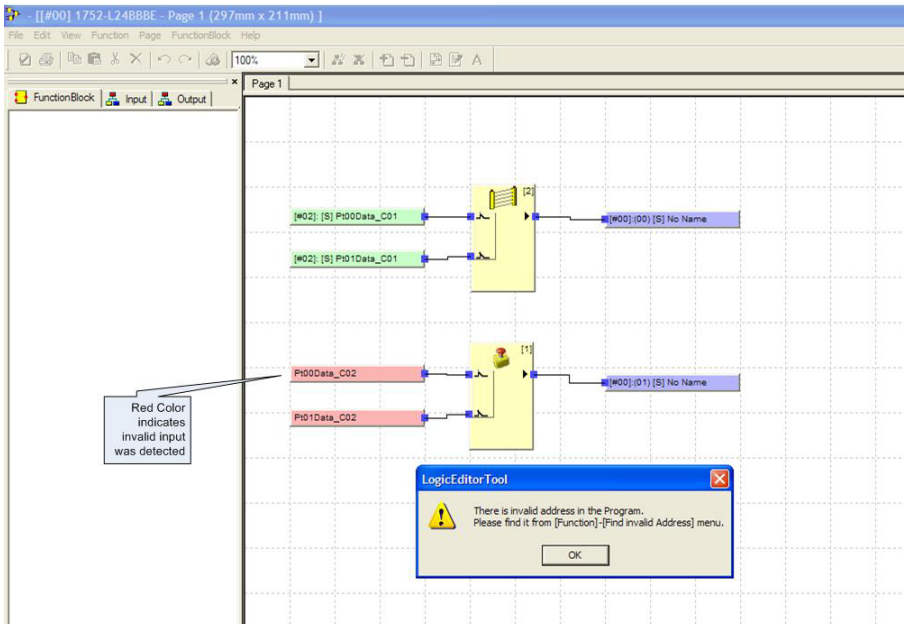
1. Evidenziare la connessione I/O che si desidera modificare o rimuovere.



2. Fare clic sul pulsante "x".

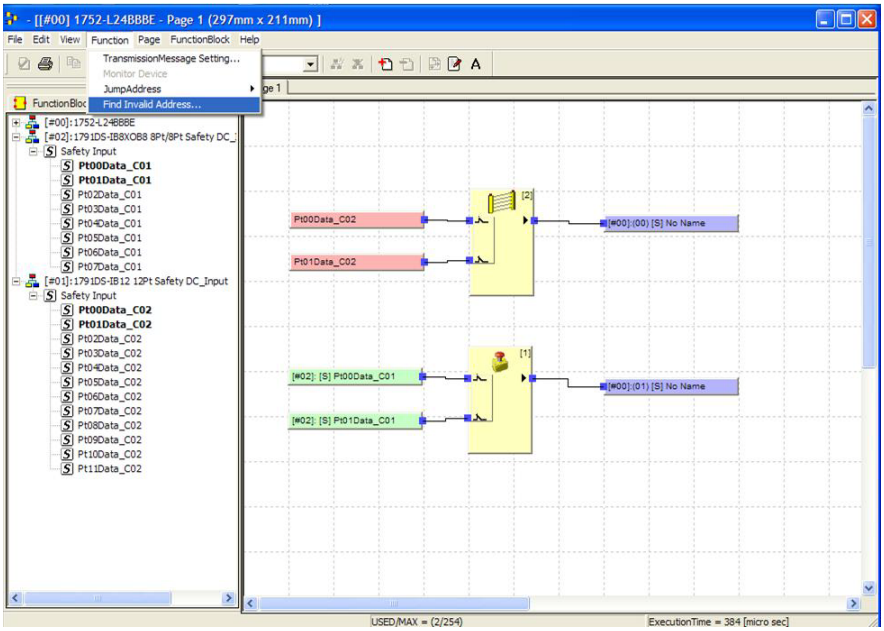
   Questo permetterà di rimuovere una connessione I/O.

In questo esempio, alla successiva visualizzazione della logica, si apre una finestra di dialogo con un messaggio di errore.

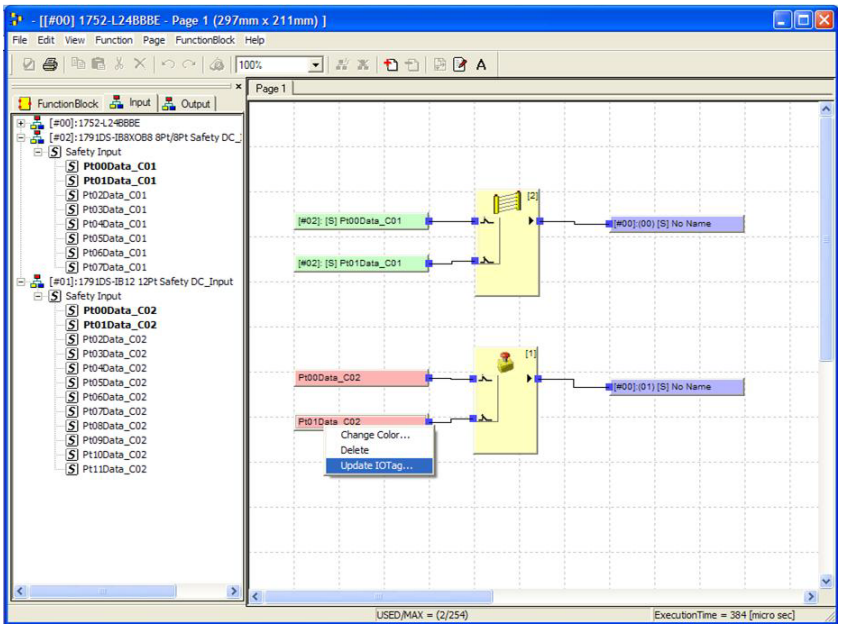


3. Fare clic su OK.

4. Per localizzare gli indirizzi non validi, selezionare Function>Find Invalid Address o localizzare tutti i tag I/O contrassegnati in rosso e fare clic con il pulsante destro del mouse su ognuno di loro.



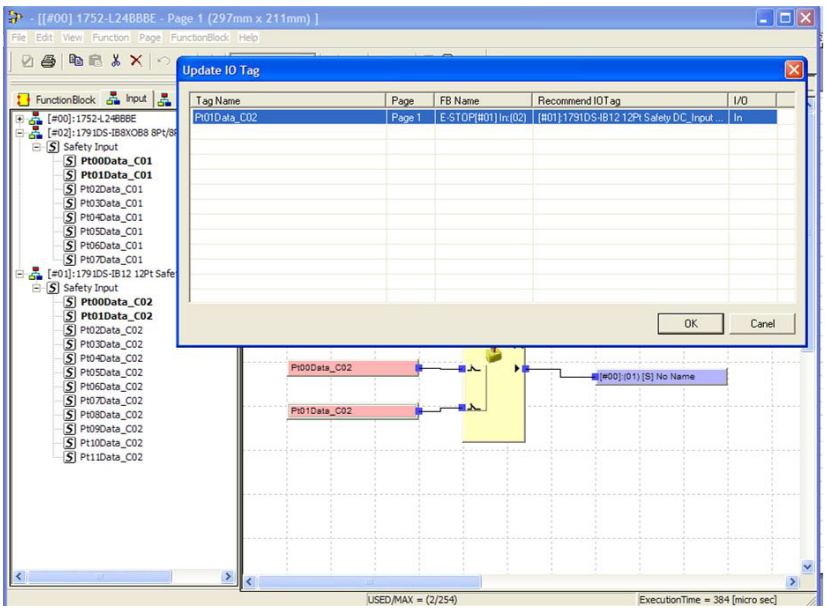
Sul tag non valido, viene visualizzato il menu a discesa.



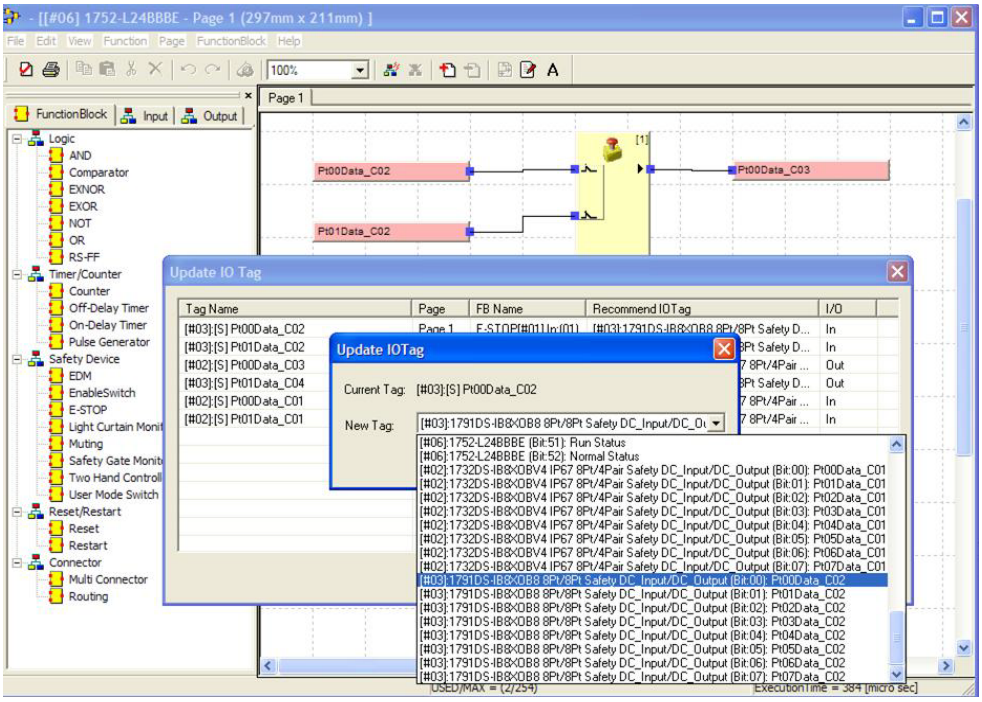
5. Fare clic con il pulsante destro del mouse sul tag non valido.

   Viene visualizzato il menu a discesa Update IO Tag.

   La finestra di dialogo visualizza l'errore del tag con il tag raccomandato. Il tag raccomandato è un suggerimento del software che considera il punto I/O a cui il tag era originariamente connesso. Occorre, comunque, verificare e confermare facendo due volte clic sull'opzione suggerita.



6. Se il tag raccomandato è corretto, evidenziare il tag e fare clic su OK. Se il tag raccomandato non è corretto, facendo due volte clic sulla riga, viene visualizzata una nuova finestra di dialogo che consente di selezionare un tag sostitutivo. È possibile anche selezionare altre opzioni.



7. Fare clic su OK.

ATTENZIONE

Se nella finestra di dialogo Update I/O Tag vengono visualizzati diversi tag, è necessario accettare tutti i tag o scegliere le alternative prima di selezionare OK. In caso contrario, verrà usato il tag I/O raccomandato.

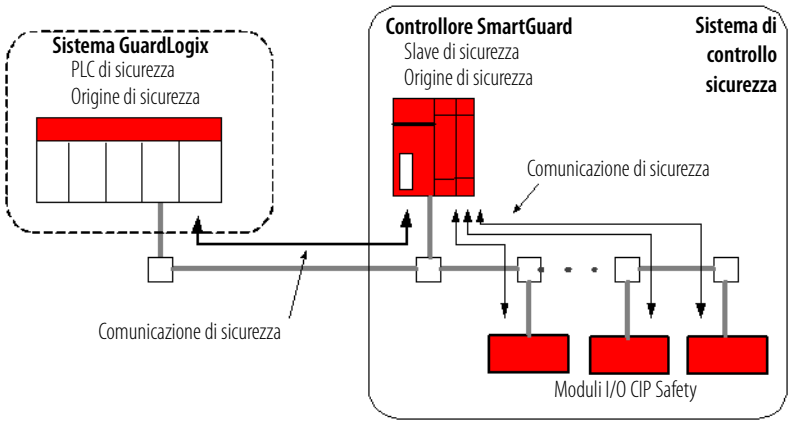
Per le raccomandazioni sulla configurazione del sistema di sicurezza, consultare il manuale di riferimento per la sicurezza “Controllori SmartGuard 600”, pubblicazione 1752-RM001B-IT-P.

Configurazione del controllore come slave di sicurezza

Come slave di sicurezza, il controllore può eseguire comunicazioni I/O di sicurezza con un massimo di 4 collegamenti, utilizzando fino a 16 byte per collegamento. I collegamenti possono essere uni-cast o multicast. Tuttavia, per 1 collegamento multicast, è possibile comunicare con un totale di 15 master.

Affinché il controllore SmartGuard esegua comunicazioni I/O di sicurezza come slave di sicurezza, è necessario creare dati I/O slave di sicurezza e configurare i collegamenti I/O di sicurezza nel master di sicurezza.

Controllore SmartGuard come slave di sicurezza ed origine di sicurezza



Quando il controllore funziona come slave di sicurezza, è possibile configurare i sistemi slave di sicurezza in modo da trasferire i dati I/O locali (dati di monitoraggio), i dati di stato del controllore e dell'I/O e i dati dell'I/O distribuito a un master di sicurezza. I dati di sicurezza possono anche essere scritti dal master di sicurezza sul controllore SmartGuard slave ed essere utilizzati nel relativo programma applicativo.

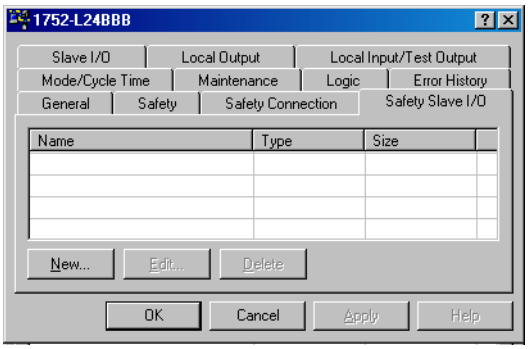
Una volta impostati i dati di stato, lo stato viene allocato all'inizio dell'area di I/O remoto, con i dati di stato che precedono i dati I/O locali. Seguono i tag I/O registrati dall'utente. Le aree di stato non impostate non sono riservate. Tutti i dati validi sono allocati senza aree non assegnate.

Creazione di dati I/O slave di sicurezza

Attenersi alla seguente procedura per creare un sistema slave di sicurezza.

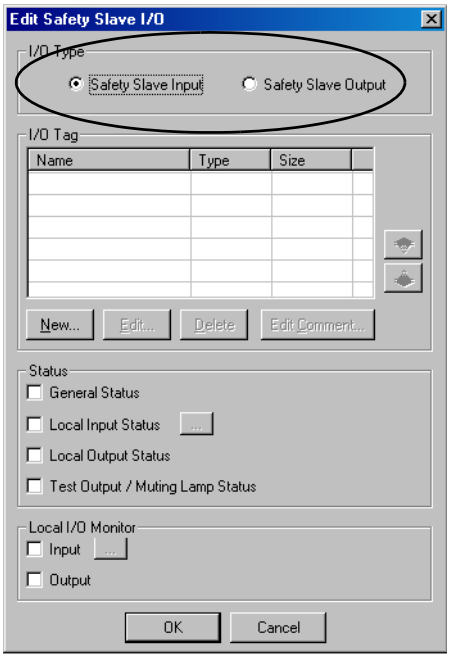
1. Nel software RSNetWorx per DeviceNet, fare clic con il pulsante destro del mouse sul controllore SmartGuard che funzionerà come slave di sicurezza, quindi selezionare Properties.

2. Fare clic sulla scheda Safety Slave I/O.



3. Fare clic su New.

4. Nella finestra di dialogo Edit Safety Slave I/O, fare clic sul tipo di I/O: Safety Slave Input o Safety Slave Output.



Tipo di I/O	Direzione dei dati di sicurezza
Safety Slave Input	Slave di sicurezza del controllore SmartGuard –> master di sicurezza
Safety Slave Output	Master di sicurezza –> slave di sicurezza del controllore SmartGuard

5. Per aggiungere informazioni di stato per i tipi di ingresso di sicurezza, selezionare la corrispondente casella di controllo Status.

Nome del tag	Dimensione dati	Tipo di attributo
General Status	Byte	Non di sicurezza
Stato degli ingressi locali	Parola	Sicurezza
Stato delle uscite locali	Byte	Sicurezza
Stato dell'uscita di test o della spia di muting	Byte	Non di sicurezza

I vari tipi di uscita di sicurezza non possono includere dati di stato. È possibile solo leggere i dati di stato; non è possibile modificarli.

6. Per aggiungere dati di controllo I/O locale per i vari tipi di ingresso di sicurezza, selezionare la casella di controllo Local I/O Monitor appropriata.

Nome del tag	Dimensione dati	Tipo di attributo
Local Input Monitor 1 (ingressi 0-7)	Byte	Sicurezza
Local Input Monitor 2 (ingressi 8-15)	Byte	Sicurezza
Local Output Monitor (uscite 0-7)	Byte	Sicurezza

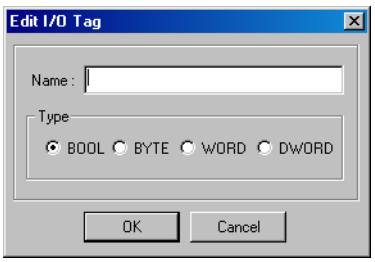
I vari tipi di uscita di sicurezza non possono includere dati di controllo I/O locale. È possibile solo leggere i valori di ingresso e di uscita, ma non è possibile sovrascriverli direttamente.

7. Fare clic su New per creare un tag I/O per il sistema di sicurezza.

   È possibile definire più tag I/O in un sistema I/O. È possibile definire tag I/O per un massimo di 16 byte in ogni sistema I/O. I tag I/O definiti in questa fase possono essere utilizzati in Logic Editor.

   Immettere punti di ingresso o uscita specifici se non si desidera condividerli tutti. È possibile condividere ingressi o uscite di I/O distribuito specificando i rispettivi nomi dei tag.

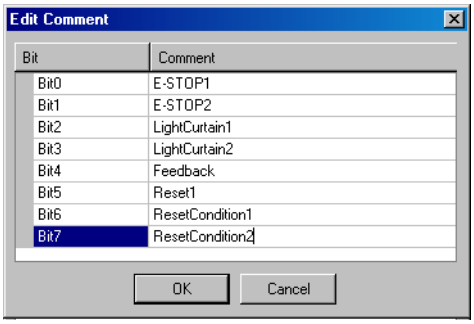
8. Immettere un nome per il tag e selezionare il tipo: BOOL, BYTE, WORD o DWORD.



9. Fare clic su OK.

10. Per creare un nome di tag per ogni bit in un sistema I/O, procedere come segue.
    a. Selezionare il sistema desiderato e fare clic su Edit Comment.

    b. Immettere un commento per ogni bit nel tag.



    I commenti immessi sul nome di tag vengono visualizzati in Logic Editor.

    c. Fare clic su OK.

11. Fare di nuovo clic su OK per tornare alla scheda Safety Slave I/O.

12. Creare altri sistemi di ingresso o di uscita slave di sicurezza, se richiesti nell'applicazione in uso, ripetendo i punti da 3 a 11.

13. Per salvare la configurazione, dal menu File, selezionare Save.

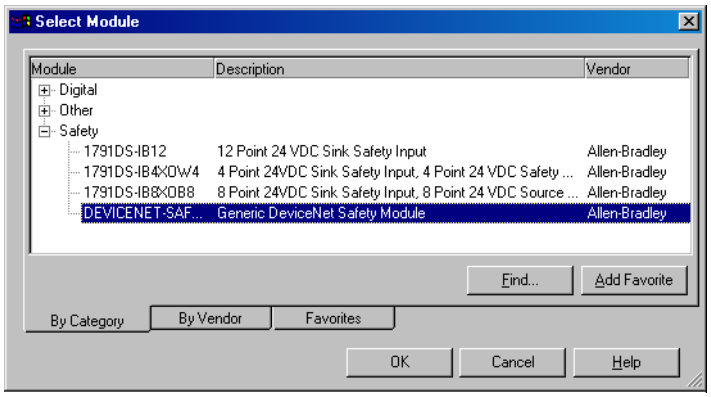
Utilizzo del profilo generico di sicurezza nel software RSLogix 5000

È possibile effettuare il collegamento al controllore slave SmartGuard utilizzando il profilo generico di sicurezza del software RSLogix 5000.

Attenersi alla seguente procedura per effettuare il collegamento al controllore.

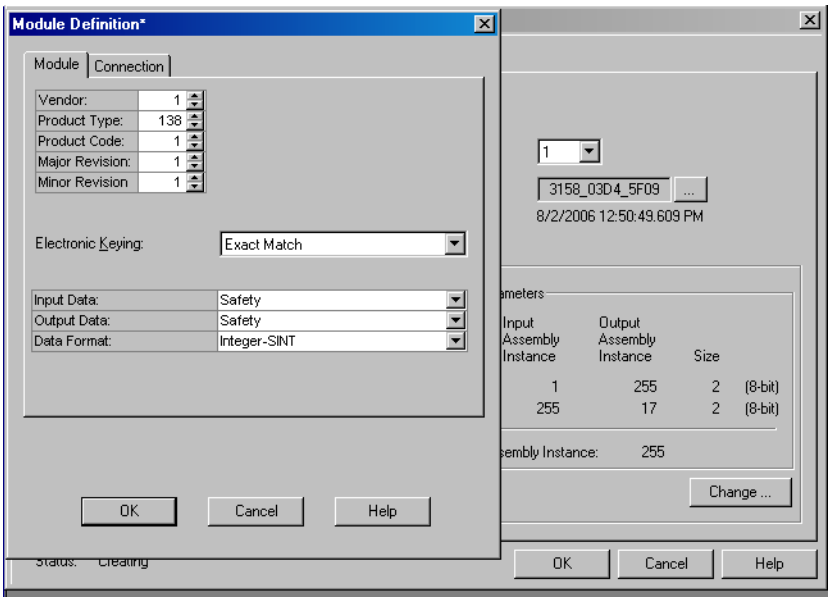
1. Nel software RSLogix 5000, fare clic con il pulsante destro del mouse sulla rete DeviceNet e selezionare New Module.

2. Selezionare Generic DeviceNet Safety Module e fare clic su OK.

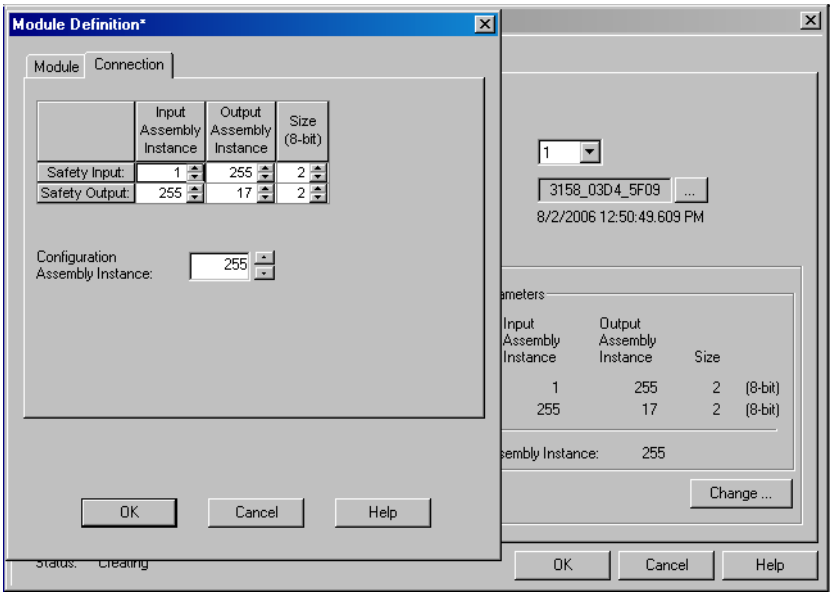


3. Nella finestra di dialogo New Module, fare clic su Change.

4. Nella finestra di dialogo Module Definition, impostare i parametri come illustrato di seguito.



5. Nella finestra di dialogo Module Definition, fare clic sulla scheda Connection.



6. Impostare i parametri per gli ingressi e le uscite di sicurezza utilizzando le seguenti tabelle.

Gruppi di ingresso

Se il nome dell'ingresso slave di sicurezza è	Impostare il numero di istanza dell'ingresso di profilo generico su	Impostare il numero di istanza dell'uscita di profilo generico su
Safety Input 1	1	255
Safety Input 2	2	255
Safety Input 3	3	255
Safety Input 4	4	255

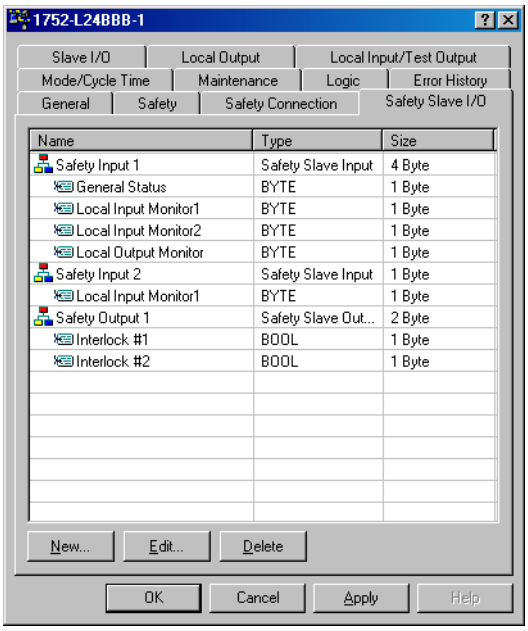
Gruppi di uscita

Se il nome dell'uscita slave di sicurezza è	Impostare il numero di istanza dell'ingresso di profilo generico su	Impostare il numero di istanza dell'uscita di profilo generico su
Safety Output 1	255	17 (per 0x11)
Safety Output 2	255	18 (per 0x12)
Safety Output 3	255	19 (per 0x13)
Safety Output 4	255	20 (per 0x14)

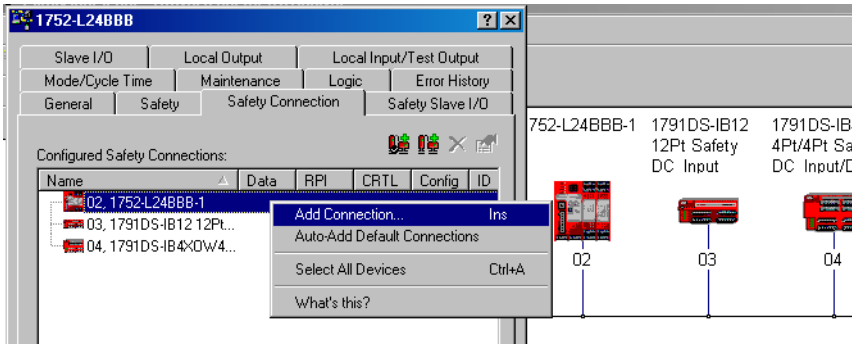
Interblocco di sicurezza tra due controllori SmartGuard

L'interblocco di sicurezza consente a due controllori SmartGuard di condividere i dati di sicurezza e prendere decisioni in base agli ingressi o alle uscite reciproche. L'interblocco di sicurezza consente di distribuire il controllo di sicurezza a più controllori SmartGuard che funzionano insieme.

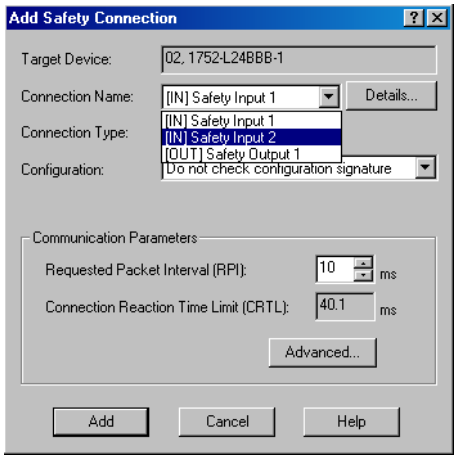
1. Configurare uno degli I/O slave di sicurezza SmartGuard come spiegato in Creazione di dati I/O slave di sicurezza a pagina 90.



2. Nella scheda Safety Connections dell'altro controllore SmartGuard, il controllore che agirà da master di sicurezza, fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Add Connection.

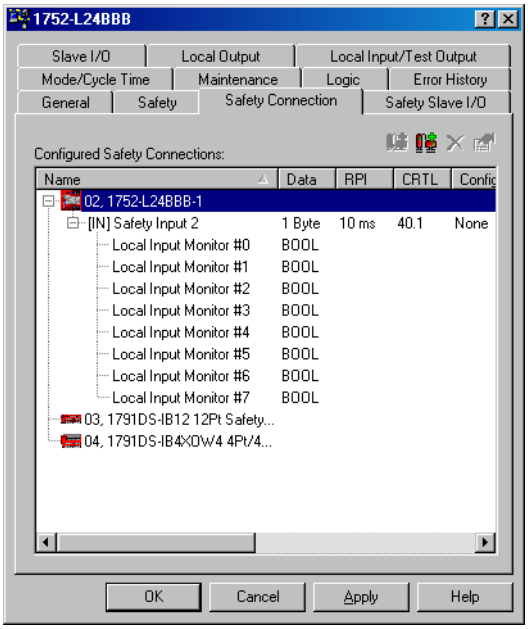


3. Dal menu a discesa Connection Name, selezionare il sistema I/O di sicurezza da utilizzare.



4. Fare clic su Add.

A questo punto, il controllore SmartGuard che agisce da master di sicurezza potrà leggere gli ingressi (0-7) dell'altro controllore SmartGuard.



Configurazione del controllore come slave DeviceNet standard

Come slave DeviceNet standard, il controllore può eseguire comunicazioni I/O standard con 1 master standard per un massimo di 2 collegamenti, utilizzando fino a 16 byte per collegamento (128 byte per i dati di ingresso della comunicazione EtherNet/IP). Il controllore SmartGuard può anche rispondere ai messaggi espliciti standard.

È possibile allocare nel master standard informazioni sullo stato interno del controllore e un'area specifica di I/O.

IMPORTANTE I dati scritti sul controllore SmartGuard tramite la relativa connessione slave standard non devono essere considerati dati di sicurezza e non devono essere utilizzati per il controllo delle funzioni di sicurezza nel programma applicativo SmartGuard.

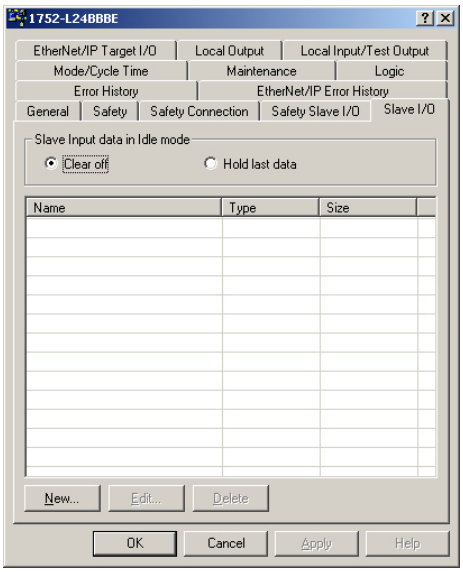
Affinché il controllore SmartGuard esegua comunicazioni I/O standard come slave standard, è necessario creare dati I/O slave standard e configurare i collegamenti I/O nel master standard.

Creazione di dati I/O slave standard

Attenersi alla seguente procedura per creare sistemi I/O slave standard.

1. Nel software RSNetWorx per DeviceNet, fare clic con il pulsante destro del mouse sul controllore SmartGuard che funzionerà come slave standard, quindi selezionare Properties.

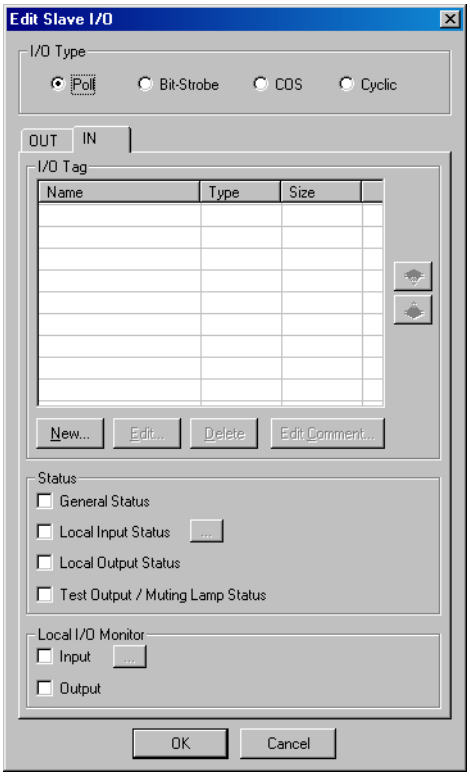
2. Fare clic sulla scheda Slave I/O.



3. Configurare il controllore slave in modo da annullare o conservare gli ultimi dati per un sistema di ingresso che il controllore slave trasmette al master standard quando:
   - la modalità del controllore slave passa da Run a riposo
   - il controllore rileva un errore, ad esempio un errore di comunicazione in una catena di sicurezza che imposta i dati su un tag I/O in un sistema di ingresso.

4. Fare clic su New.

5. Fare clic sul tipo di I/O: Poll, Bit-Strobe, COS o Cyclic.



I dati di uscita non possono utilizzare un tipo di collegamento bit strobe poiché non vengono emessi dati bit strobe dal master standard. Inoltre, la dimensione massima per l'ingresso di dati bit strobe nel master standard è di 8 byte. Non è possibile utilizzare contemporaneamente i collegamenti COS e ciclico.

6. Per aggiungere informazioni di stato per i tipi di ingresso, selezionare le caselle di controllo Status (opzionale).

   Se il tipo di I/O è Input, è possibile includere le seguenti informazioni sullo stato nel sistema I/O.

Nome del tag	Dimensione dati	Tipo di attributo
General Status	Byte	Non di sicurezza
Stato degli ingressi locali	Parola	Non di sicurezza
Stato delle uscite locali	Byte	Non di sicurezza
Stato dell'uscita di test o della spia di muting	Byte	Non di sicurezza

7. Per aggiungere dati di controllo I/O locale per i vari tipi di ingresso, selezionare la casella di controllo Local I/O Monitor appropriata.

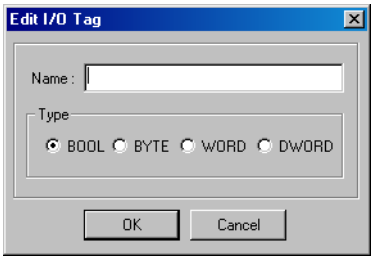
Nome del tag	Dimensione dati	Tipo di attributo
Local Input Monitor 1 (ingressi 0-7)	Byte	Non di sicurezza
Local Input Monitor 2 (ingressi 8-15)	Byte	Non di sicurezza
Local Output Monitor (uscite 0-7)	Byte	Non di sicurezza

I vari tipi di uscita non possono includere dati di controllo I/O locale. È possibile solo leggere i valori di ingresso e di uscita, ma non è possibile sovrascriverli direttamente.

8. Fare clic su New per creare un tag I/O.

È possibile definire più tag I/O in un sistema I/O. È possibile definire tag I/O per un massimo di 16 byte in ogni sistema I/O. I tag I/O definiti in questa fase possono essere utilizzati in Logic Editor.

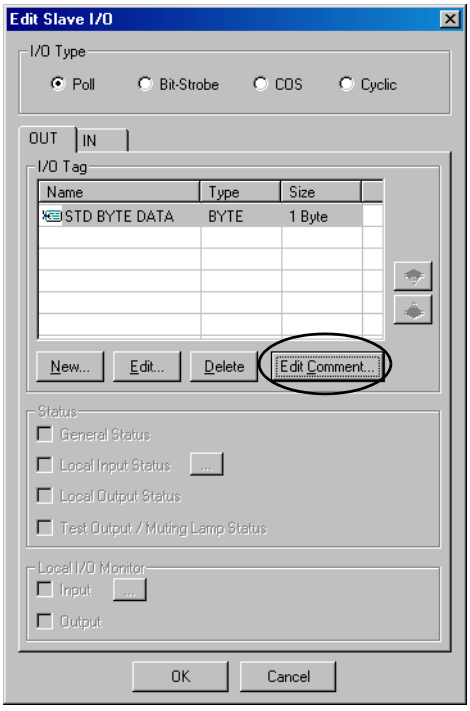
9. Immettere un nome per il tag e fare clic sul tipo: BOOL, BYTE, WORD o DWORD.



10. Fare clic su OK.

11. Per creare un nome di tag per ogni bit in un sistema I/O, procedere come segue.

a. Selezionare il sistema desiderato e fare clic su Edit Comment.



b. Immettere un commento per ogni bit nel tag.

I commenti immessi sul nome di tag vengono visualizzati in Logic Editor.

c. Fare clic su OK.

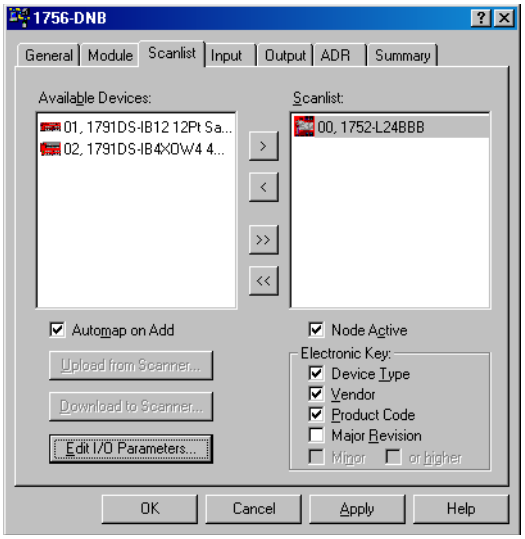
12. Fare di nuovo clic su OK per tornare alla scheda Slave I/O.

13. Creare altri sistemi di ingresso o di uscita slave, se richiesti nell'applicazione in uso, ripetendo i punti da 4 a 12.

14. Dal menu File, selezionare Save per salvare la configurazione.

Aggiunta di uno slave standard SmartGuard all'elenco dei dispositivi del master standard

Per rendere disponibili i sistemi I/O slave standard per il master standard, aggiungere il controllore slave standard SmartGuard all'elenco dei dispositivi del master.



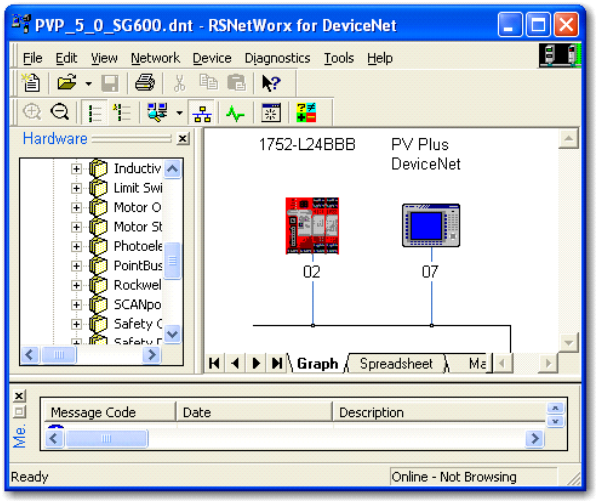
Per informazioni sulla configurazione di dispositivi specifici, consultare la documentazione del master standard in uso.

Salvare la configurazione nel software RSNetWorx per DeviceNet selezionando File>Save.

Lettura e scrittura tra il controllore SmartGuard e un'interfaccia PanelView Plus

Questa sezione spiega come eseguire le operazioni di lettura e scrittura tra il controllore SmartGuard e l'interfaccia PanelView Plus. Nell'ambito di questa architettura, il controllore SmartGuard è uno slave standard. Vedere a pagina 98 per ulteriori informazioni.

Controllore SmartGuard e interfaccia PanelView Plus in rete

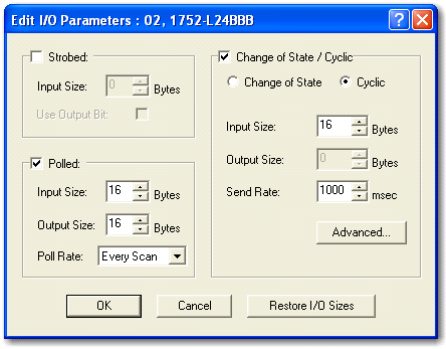


Tra i quattro tipi di connessione disponibili, è possibile selezionare fino a due connessioni ma una sola connessione per ogni tipo. Ad esempio, sono possibili una connessione di polling e 1 connessione COS ma non due connessioni di polling. Sia il polling che la modalità COS/ciclica ammettono ingressi e uscite (lettura e scrittura) in un'unica connessione.

Una connessione di polling che usa sia ingressi che uscite può avere 16 byte di dati di ingresso e 16 byte di dati di uscita. Se si aggiunge un'altra connessione, è possibile avere 16 byte aggiuntivi di dati.

Se si usa la connessione di polling e poi si aggiunge una connessione COS/ciclica, l'uscita non è disponibile. La massima configurazione dei dati è illustrata di seguito.

Finestra di dialogo Edit I/O Parameters



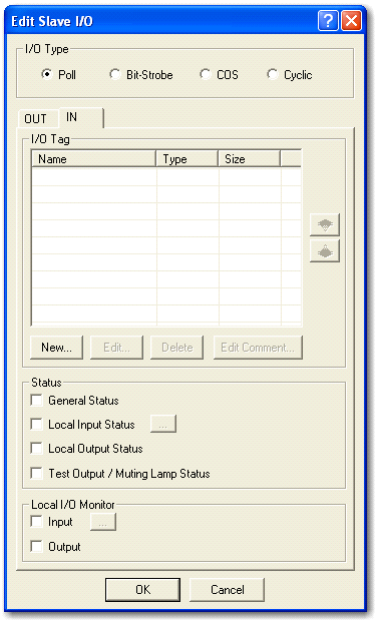
Questa configurazione permette 32 byte di dati di ingresso (16 via polling e 16 via COS o ciclica) e 16 byte di dati di uscita attraverso la connessione di polling. Questa configurazione è descritta più ampiamente in questo capitolo.

Lettura dati BOOL dal controllore SmartGuard e loro visualizzazione sull'interfaccia PanelView Plus

Per leggere i dati BOOL dal controllore SmartGuard e visualizzarli sull'interfaccia PanelView Plus, procedere come segue.

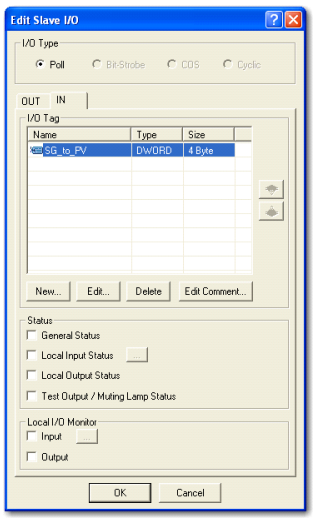
1. Aprire il software RSNetWorx.
2. Aprire "SmartGuard properties".
3. Fare clic sulla scheda Slave I/O.

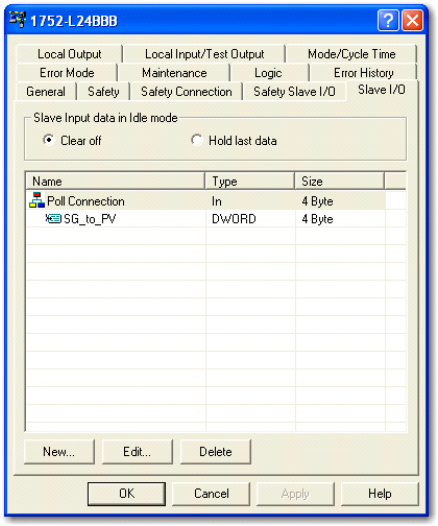
   Viene visualizzata la seguente finestra di dialogo.



4. Fare clic sulla scheda IN.
5. Inserire i nomi dei tag che saranno letti dall'interfaccia PanelView Plus.

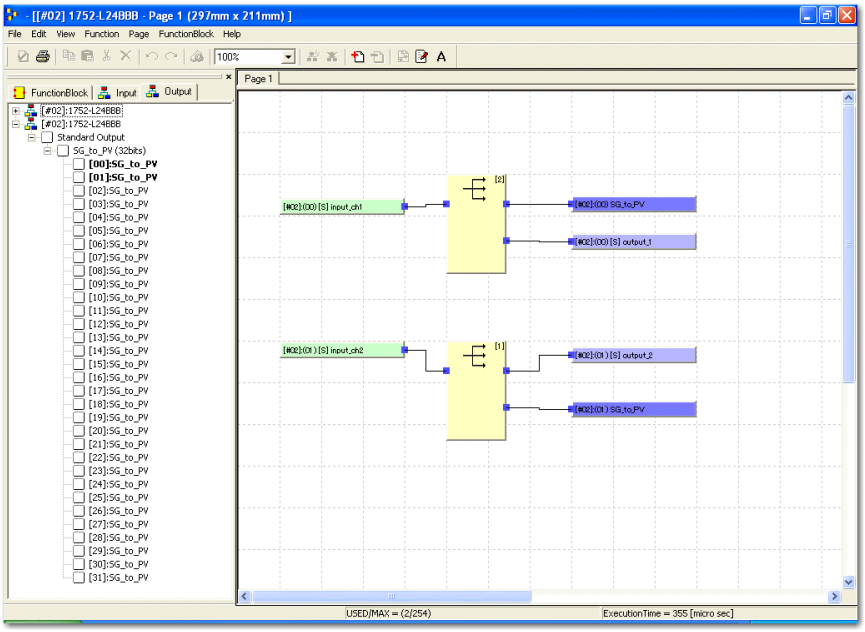
In questo caso, è stato creato un singolo tag da 4 byte che userà una connessione di polling. Questi 4 byte vengono letti dall'interfaccia PanelView Plus.





Anche se è stato creato un tag DWORD, è possibile accedere a tutti i 32 bit del DWORD nell'editor SmartGuard. Il codice campione SmartGuard controlla due dei 32 bit.

I tag in grassetto nell'elenco dei tag sono utilizzati nel codice.



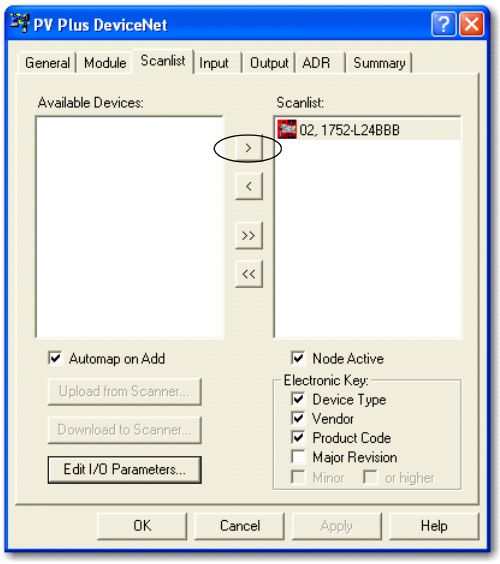
6. Scaricare la configurazione nel controllore SmartGuard 600.

Configurazione dell'elenco di scansione dello scanner PanelView

Per configurare l'elenco di scansione dello scanner PanelView Plus DeviceNet, procedere come segue.

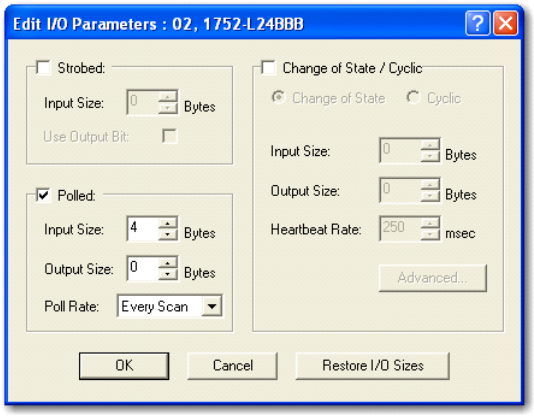
1. Fare clic sulla scheda Scanlist.

2. Fare clic sulla freccia a destra per spostare il controllore SmartGuard nell'elenco di scansione.



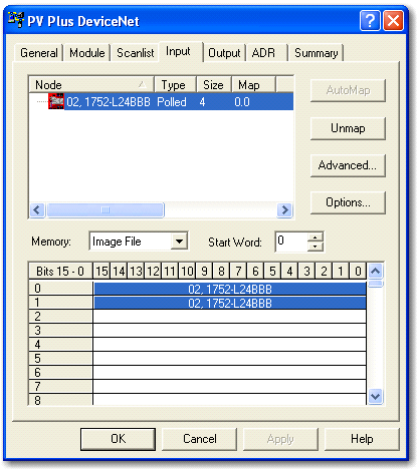
3. Fare clic su Edit I/O Parameters e verificare che sia configurata come illustrato di seguito.

   L'esempio ha una connessione di polling a 4 byte che sarà un ingresso all'interfaccia PanelView Plus.



   Essendo stato selezionato Automap on Add, la seguente mappatura viene generata automaticamente.

4. Verificare che i 4 byte di dati di ingresso siano mappati come illustrato.



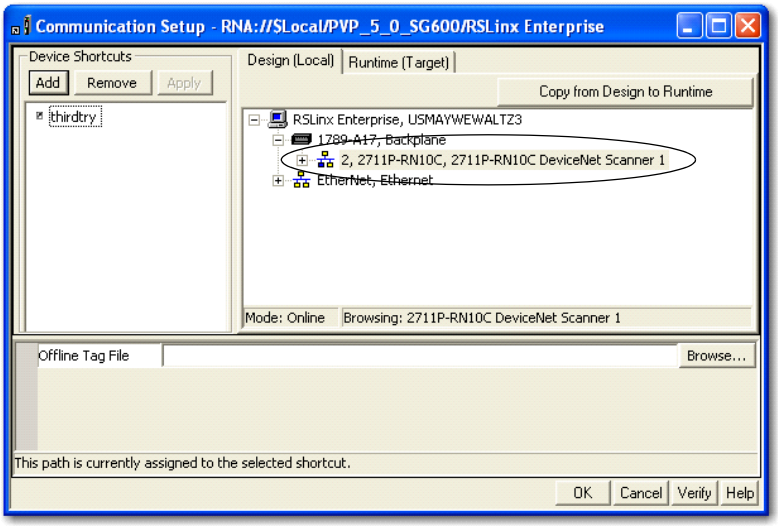
5. Fare clic con il pulsante destro del mouse sull'interfaccia PanelView Plus nel software RSNetWorx e selezionare Download to Device.

Configurazione dello scanner RN10C DeviceNet

Per configurare lo scanner RN10C DeviceNet, procedere come segue.

La scorciatoia nel software RSLinx Enterprise dovrebbe essere simile a quella illustrato.

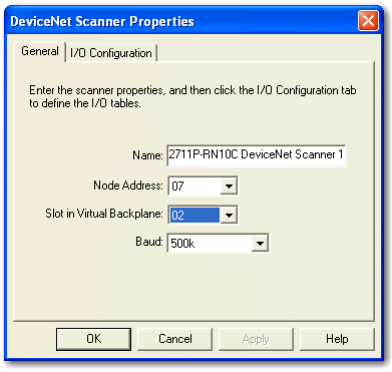
Prendere nota che il numero di slot dello scanner RN10C è 2.



1. Fare clic con il pulsante destro del mouse sullo scanner RN10C e selezionare Properties.

2. Inserire il nome dello scanner.

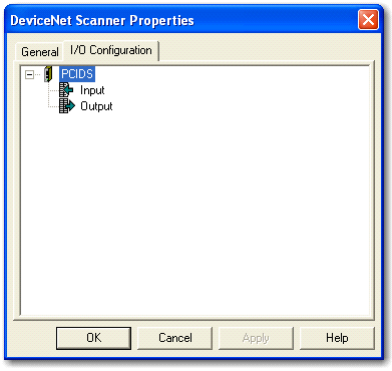
3. Dal menu a discesa corrispondente, selezionare Node Address, Slot in the Virtual Backplane e Baud rate.



L'interfaccia PanelView Plus è configurata per DeviceNet nodo 7. Il controllore SmartGuard ha i microinterruttori impostati per l'autorilevamento (sinistra/sinistra/sinistra/destra dall'alto in basso). Scegliere la velocità di trasmissione più adatta all'applicazione.

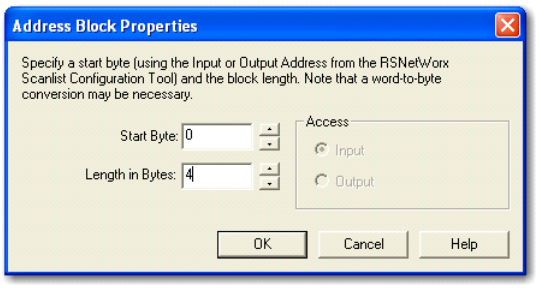
4. Fare clic sulla scheda I/O Configuration.

Viene visualizzata la seguente finestra di dialogo.



5. Fare clic con il pulsante destro del mouse su Input e selezionare Add Address Block.

Viene visualizzata la seguente finestra di dialogo.

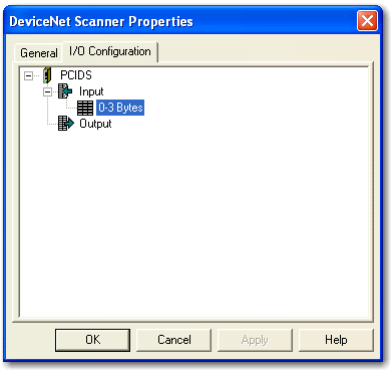


6. Inserire 4 come Length in Bytes.

Questo corrisponderà a quello che lo scanner legge dal controllore SmartGuard.

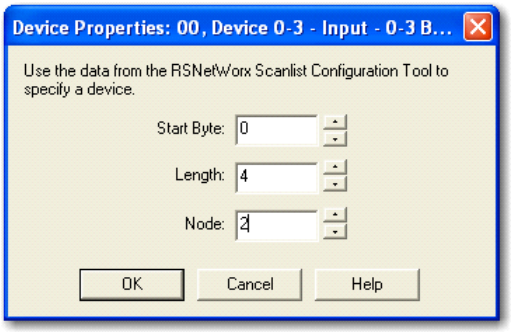
7. Fare clic su OK.

   Viene visualizzata la configurazione I/O.



8. Fare clic con il pulsante destro del mouse su 0-3 Bytes e selezionare Add Devices.

   Viene visualizzata la seguente finestra di dialogo.

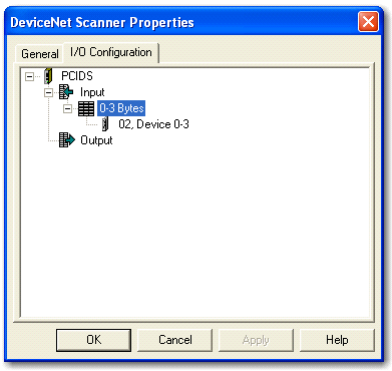


9. Impostare il numero di nodo in modo che corrisponda a quello del controllore SmartGuard.

   Il numero di nodo in questo esempio è 2.

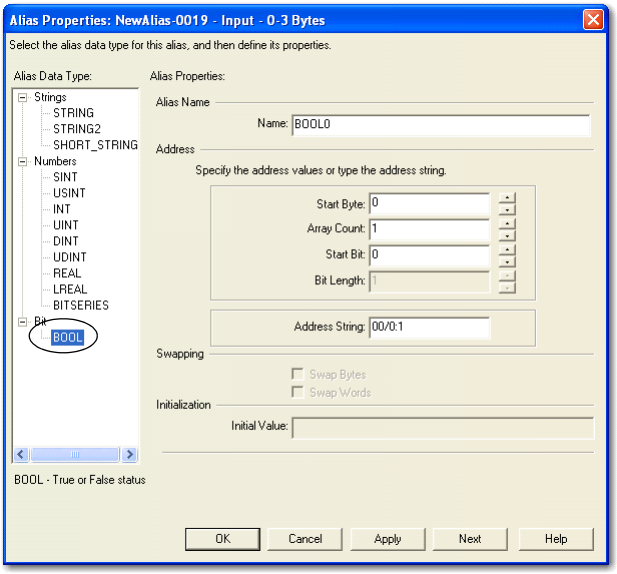
10. Fare clic su OK.

    Viene visualizzata la seguente finestra di dialogo.



11. Fare clic con il pulsante destro del mouse su 0-3 Bytes e selezionare Add Alias.

    Viene visualizzata la seguente finestra di dialogo.



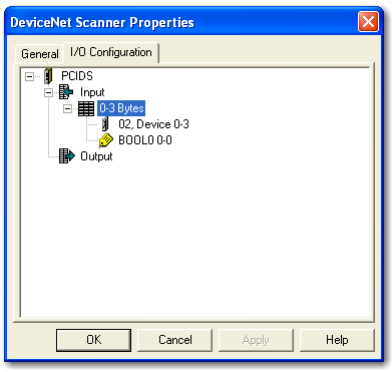
12. Selezionare il tipo di dati in grassetto (BOOL) e, dal corrispondente menu a discesa, selezionare Start Byte, Array Count e Start Bit.

    I valori sopra riportati rappresentano il bit 0 del primo byte.

13. Inserire il nome.

14. Fare clic su OK.

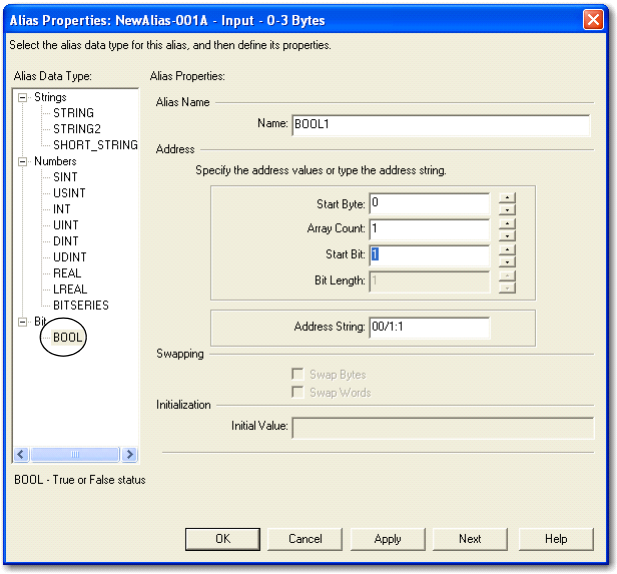
Viene visualizzata la seguente finestra di dialogo.



Per aggiungere un secondo tipo di dati BOOL che rappresenti il bit 1 del primo byte, procedere come segue.

1. Fare clic con il pulsante destro del mouse su 0-3 Bytes e selezionare Add Alias.

   Una volta selezionato il tipo di dati BOOL, viene visualizzata la seguente finestra di dialogo.

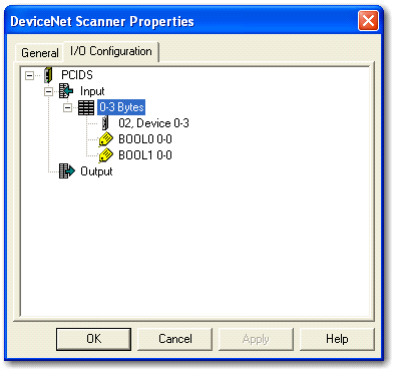


2. Dal menu a discesa corrispondente, selezionare Start Byte, Array Count e Start Bit.

3. Inserire il nome.

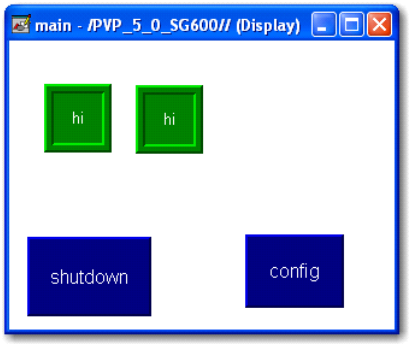
4. Fare clic su OK.

   Viene visualizzata la seguente finestra di dialogo.

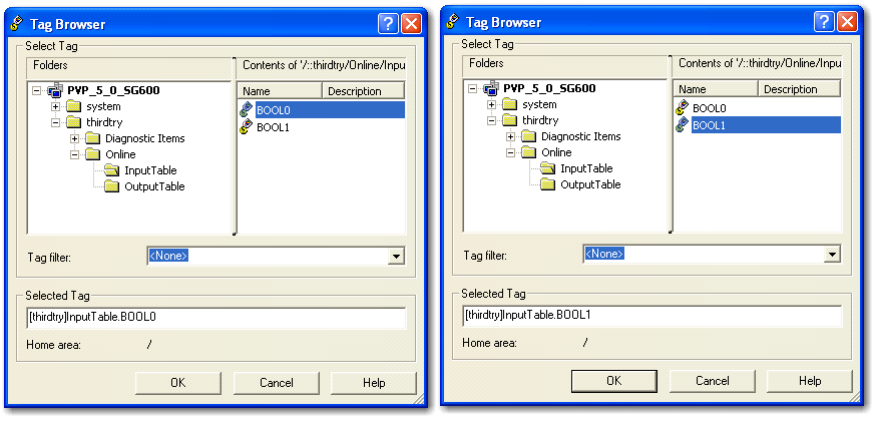


5. Fare clic su OK.

Il passo finale consiste nel creare la grafica PanelView Plus che legge i tag alias. Questo esempio usa due indicatori multistato che leggono i due alias.



I tag di ognuno degli indicatori multistato possono essere esplorati mediante il software RSLinx Enterprise. Selezionare i tag come illustrato.



Infine, è necessario salvare il progetto, generare un file di runtime e scaricarlo nell'interfaccia PanelView Plus.

Lettura e scrittura tra il controllore SmartGuard e l'interfaccia PanelView Plus, simultaneamente

Questo esempio spiega come utilizzare due pulsanti stabili su uno schermo PanelView Plus per controllare due tag nel controllore SmartGuard 600. Per far questo, l'interfaccia PanelView Plus invia un singolo byte di dati al controllore SmartGuard. BOOL non esiste né nelle proprietà dello scanner PanelView Plus né nel controllore SmartGuard. Anche se si crea un tag BOOL nel controllore SmartGuard per accettare i dati dall'interfaccia PanelView Plus, userà comunque un byte di dati.

Nel controllore SmartGuard, non ci sono neanche valori interi a cui si possa accedere in modo programmatico. Dato che al controllore SmartGuard vengono inviati solo i valori dei dati booleani e dato che il più piccolo tipo di dati nel controllore SmartGuard è un byte, non ci sono ragioni per inviare meno di un byte dall'interfaccia PanelView Plus al controllore SmartGuard, anche se si utilizza solo una coppia di bit. Questo esempio configura un byte di dati di uscita che deve essere inviato al controllore SmartGuard ma usa solo due pulsanti. Se dall'interfaccia PanelView Plus occorre inviare più di otto BOOL al controllore SmartGuard, fare riferimento all'esempio che segue e modificare 1 byte con *x* byte nei parametri di uscita.

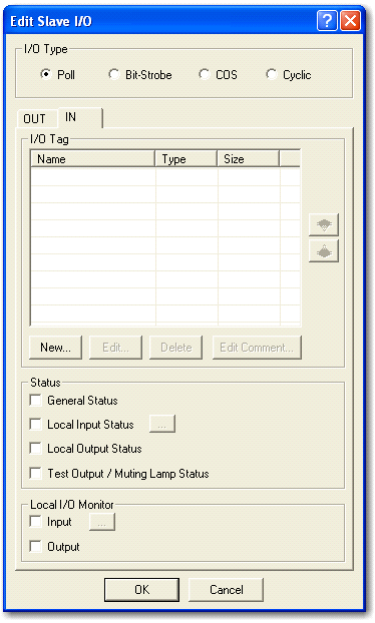
I tag che vengono letti dall'interfaccia PanelView Plus dovrebbero essere inseriti nella scheda IN.

I tag che vengono scritti dall'interfaccia PanelView Plus dovrebbero essere inseriti nella scheda OUT.

Per eseguire le operazioni di lettura e scrittura tra il controllore SmartGuard e l'interfaccia PanelView Plus in modo simultaneo, procedere come segue.

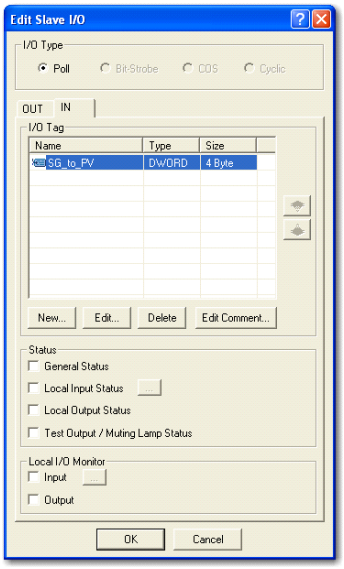
1. Aprire il software RSNetWorx.
2. Aprire "SmartGuard properties".
3. Fare clic sulla scheda Slave I/O.

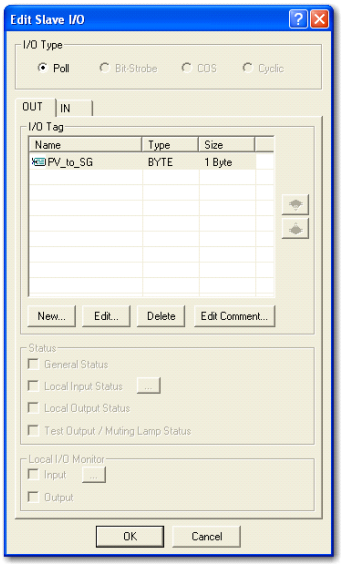
Viene visualizzata la seguente finestra di dialogo.

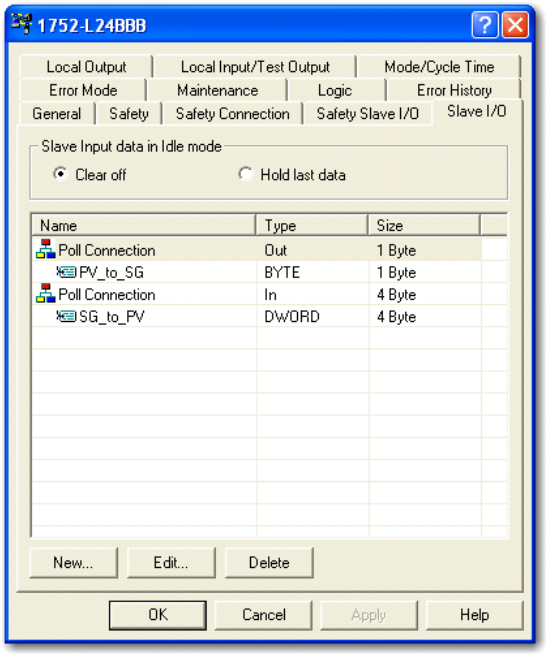


4. Fare clic sulla scheda IN.
5. Inserire i nomi dei tag che saranno letti dall'interfaccia PanelView Plus.
6. Fare clic sulla scheda OUT.
7. Inserire i nomi dei tag che saranno scritti dall'interfaccia PanelView Plus.

In questo caso, si utilizza una connessione di polling con 4 byte che possono essere letti e 1 byte che può essere scritto.



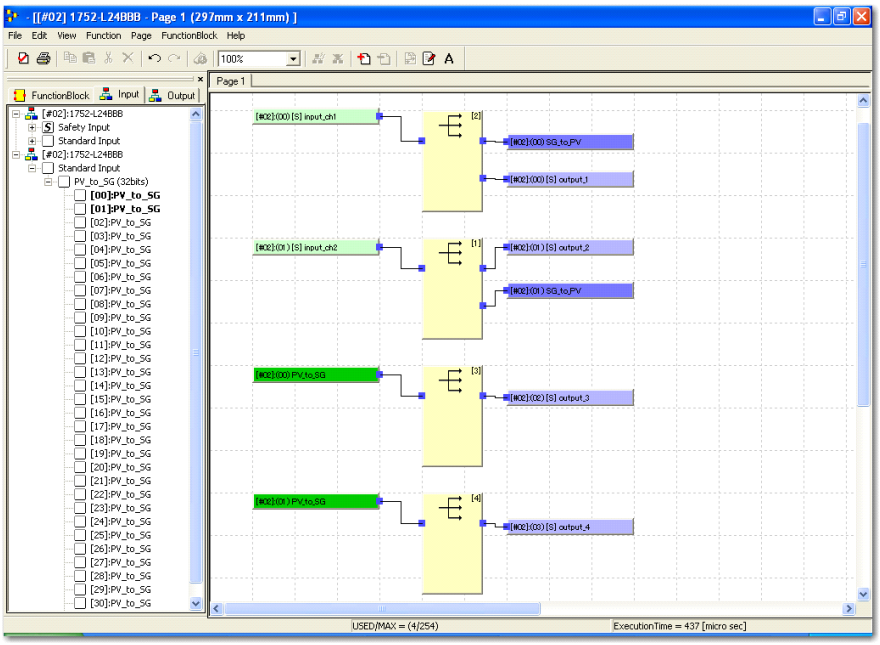




È possibile anche accedere a tutti i bit di DWORD e BYTE nell'editor SmartGuard. Il codice campione SmartGuard utilizza due bit in entrambi i buffer.

I quattro tag in grassetto nell'elenco dei tag sono utilizzati nel codice.

Di seguito, è illustrata la scheda Input attraverso cui è possibile visualizzare i tag PV_to_SG. Per visualizzare i tag SG_to_PV, fare clic sulla scheda Output.



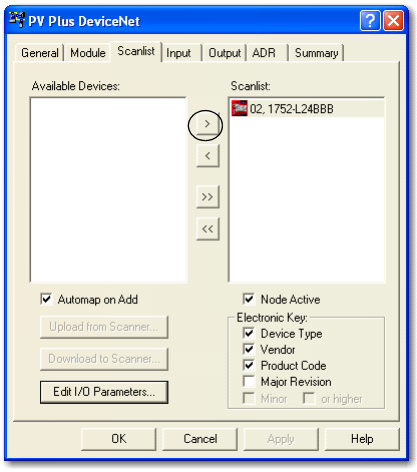
8. Scaricare la configurazione nel controllore SmartGuard 600.

Configurazione dell'elenco di scansione dello scanner PanelView

Per lo scanner PanelView Plus DeviceNet, è necessario configurare l'elenco di scansione.

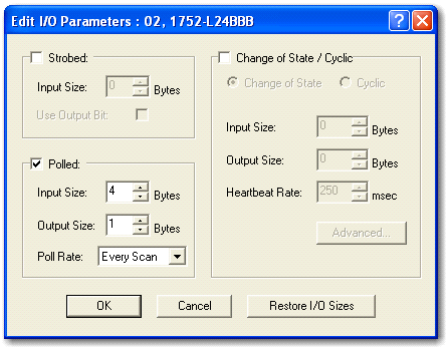
Per aggiungere il controllore SmartGuard 600 all'elenco di scansione, procedere come segue.

1. Fare clic sulla scheda Scanlist.
2. Fare clic sulla freccia a destra per spostare il controllore SmartGuard nell'elenco di scansione.



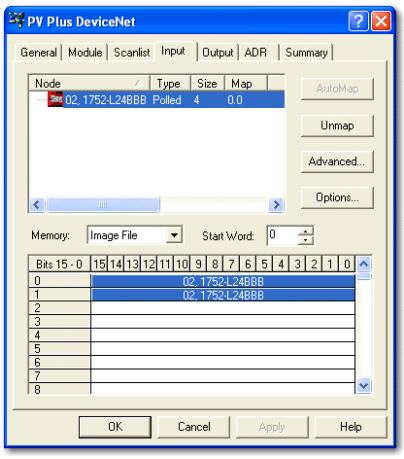
3. Fare clic su Edit I/O Parameters e verificare che sia configurato come illustrato di seguito.

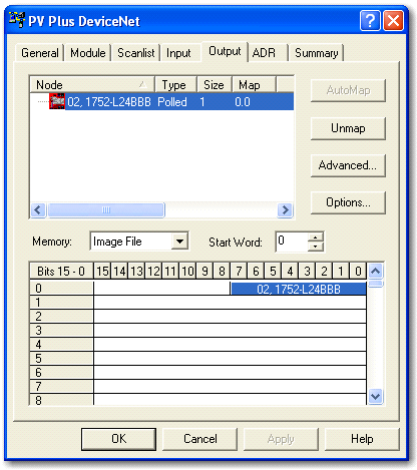
   L'esempio prevede una connessione di polling che leggerà 4 byte e scriverà 1 byte tra il controllore SmartGuard e l'interfaccia PanelView Plus.



   Essendo stato selezionato Automap on Add, la seguente mappatura viene generata automaticamente.

4. Verificare che i 4 byte di dati di ingresso ed il singolo byte di dati di uscita siano mappati come illustrato.



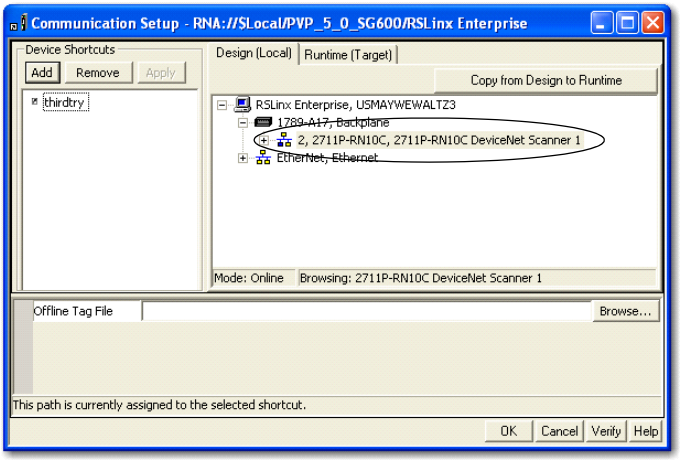


5. Nel software RSNetWorx, fare clic con il pulsante destro del mouse sull'interfaccia PanelView Plus e selezionare Download to Device per scaricare questa configurazione nell'interfaccia PanelView Plus.

Configurazione dello scanner RN10C DeviceNet

Per configurare lo scanner RN10C DeviceNet, procedere come segue.

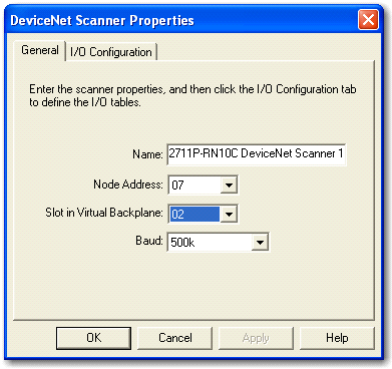
La scorciatoia nel software RSLinx Enterprise dovrebbe essere simile a quanto illustrato.



Prendere nota che il numero di slot dello scanner RN10C è 2.

1. Fare clic con il pulsante destro del mouse sullo scanner RN10C e selezionare Properties.

   Viene visualizzata la seguente finestra di dialogo.



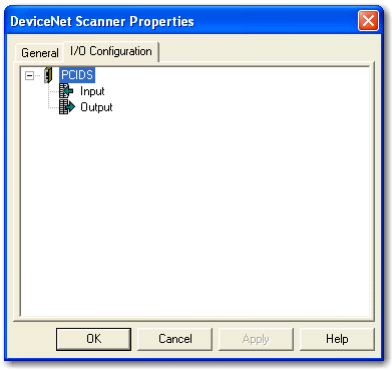
2. Inserire il nome dello scanner.

3. Dal menu a discesa corrispondente, selezionare Node Address, Slot in the Virtual Backplane e Baud rate.

   L'interfaccia PanelView Plus è configurata per DeviceNet nodo 7.
   Il controllore SmartGuard ha i microinterruttori impostati per l'autorilevamento (sinistra/sinistra/sinistra/destra dall'alto in basso).
   Scegliere la velocità di trasmissione più adatta all'applicazione.

4. Fare clic sulla scheda I/O Configuration.

Viene visualizzata la seguente finestra di dialogo.



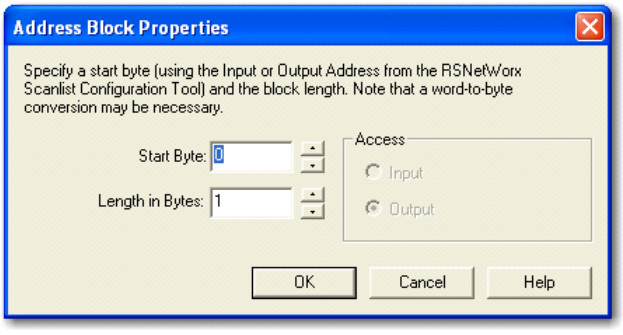
La configurazione del blocco di ingresso è trattata nella sezione “Modalità di lettura dei tipi di dati BOOL” di questo documento. Fare riferimento a quella sezione per configurare i dati che saranno letti dal controllore SmartGuard e visualizzati sull’interfaccia PanelView Plus.

Configurazione dei dati scritti dall’interfaccia PanelView Plus nel controllore SmartGuard

Per configurare i dati scritti dall’interfaccia PanelView Plus nel controllore SmartGuard, procedere come segue.

1. Fare clic con il pulsante destro del mouse su Output e selezionare Add Address Book.

   Viene visualizzata la seguente finestra di dialogo.

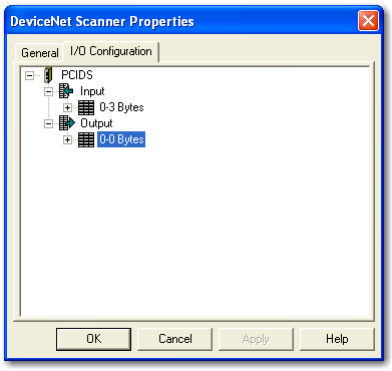


2. Inserire 1 in Length in Bytes.

   Questo corrisponderà a quello che lo scanner scrive nel controllore SmartGuard.

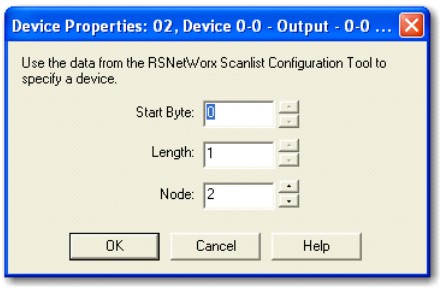
3. Fare clic su OK.

Viene visualizzata la seguente finestra di dialogo.



4. Fare clic con il pulsante destro del mouse su 0-0 Bytes e selezionare Add Devices.

   Viene visualizzata la seguente finestra di dialogo.

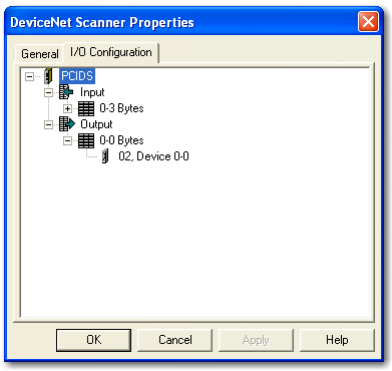


5. Impostare il numero di nodo in modo che corrisponda a quello del controllore SmartGuard.

   Il numero di nodo in questo esempio è 2.

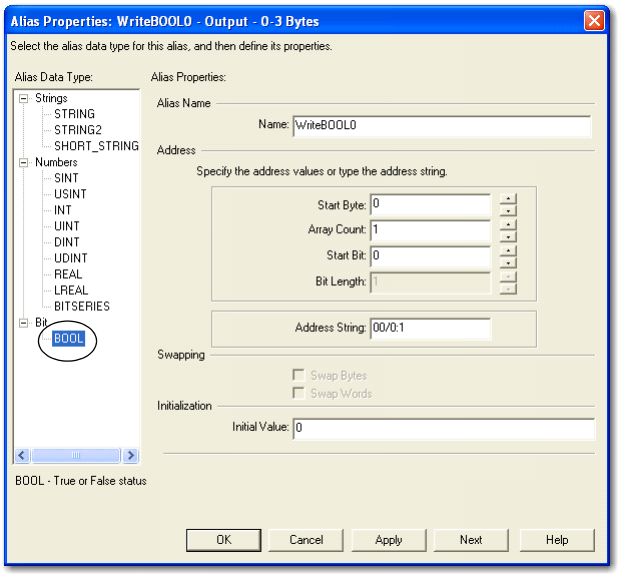
6. Fare clic su OK.

   Viene visualizzata la seguente finestra di dialogo.



7. Fare clic con il pulsante destro del mouse su 0-0 Bytes e selezionare Add Alias.

Una volta selezionato il tipo di dati BOOL, viene visualizzata la seguente finestra di dialogo.



I valori sopra riportati rappresentano il bit 0 del primo byte.

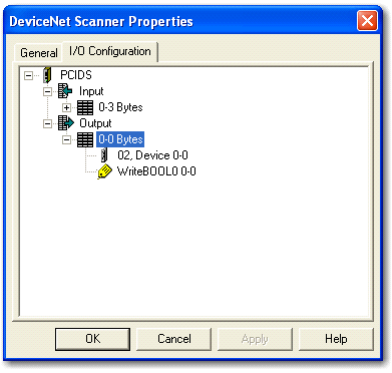
8. Dal menu a discesa corrispondente, selezionare Start Byte, Array Count e Start Bit.

9. Inserire il nome.

10. Inserire il valore iniziale di 0.

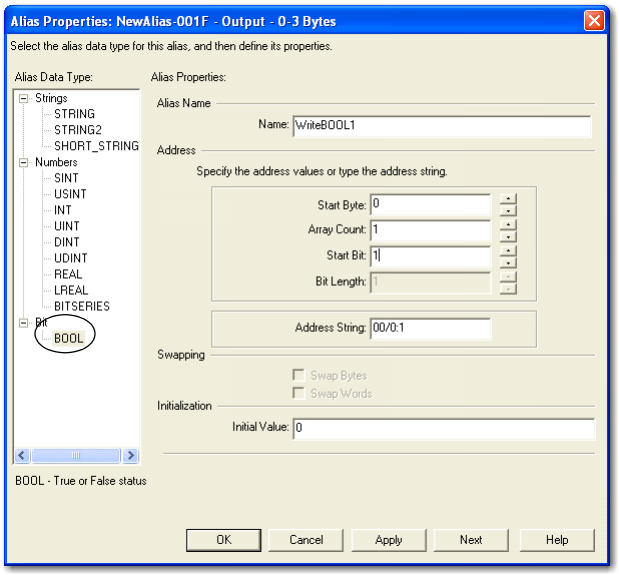
11. Fare clic su OK.

    Viene visualizzata la seguente finestra di dialogo.



Per aggiungere un secondo tipo di dati BOOL che rappresenti il bit 1 del primo byte, procedere come segue.

1. Fare clic con il pulsante destro del mouse su 0-0 Bytes e selezionare Add Alias.



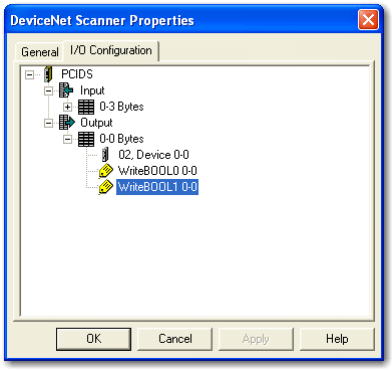
2. Selezionare il tipo di dati BOOL e, dal corrispondente menu a discesa, selezionare Start Byte, Array Count e Start Bit.

3. Inserire il nome.

4. Inserire il valore iniziale di 0.

5. Fare clic su OK.

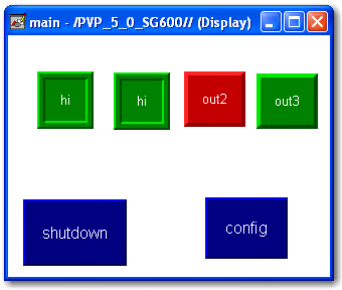
   Viene visualizzata la seguente finestra di dialogo.



6. Fare clic su OK.

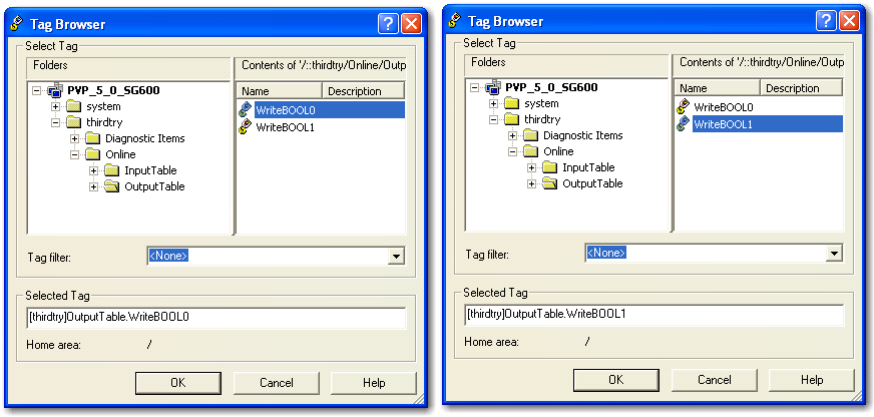
Il passo finale consiste nel creare la grafica PanelView Plus che legge i tag alias. Questo esempio prevede 2 pulsanti stabili che leggono i 2 alias.

Grafica di PanelView Plus



I tag di ognuno dei pulsanti stabili possono essere esplorati mediante il software RSLinx Enterprise. Selezionare i tag come illustrato.

Esplorazione dei tag per i pulsanti stabili



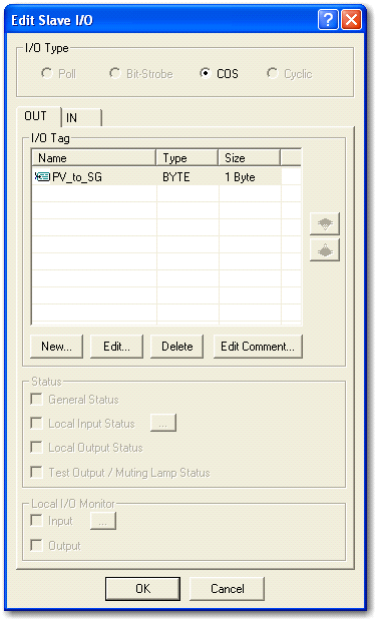
Infine, è necessario salvare il progetto, generare un file di runtime e scaricarlo nell'interfaccia PanelView Plus.

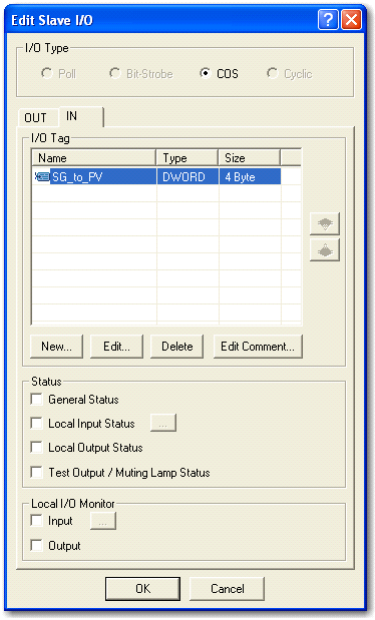
Confronto tra COS e polling

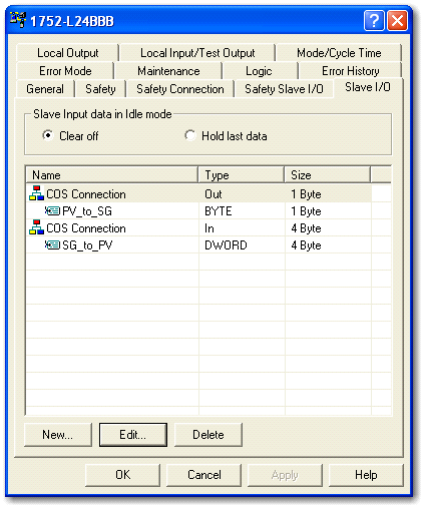
Per usare la modalità COS (Change of State, cambio di stato) anziché il polling, apportare le necessarie modifiche da pagina 113 fino a questa sezione, come illustrato dalle seguenti finestre di dialogo.

Nella configurazione I/O dello slave SmartGuard avvengono le seguenti modifiche.

Modifiche della configurazione I/O dello slave SmartGuard

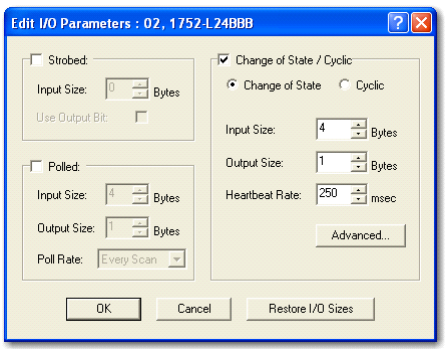


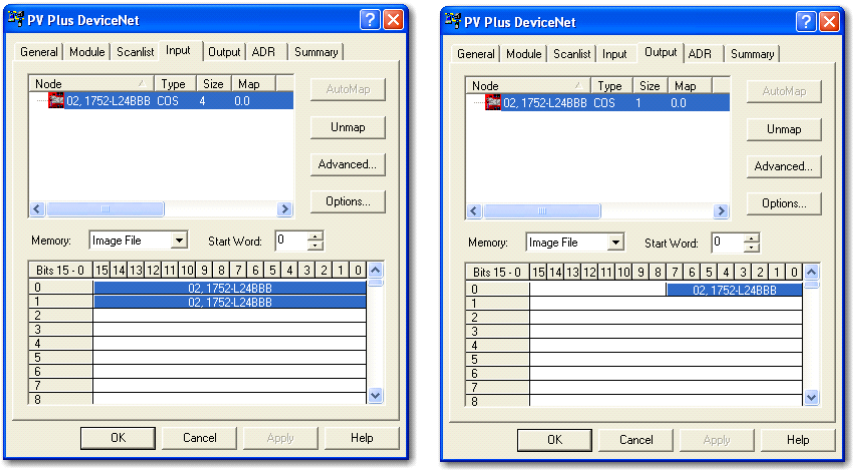




Nella configurazione dello scanner RN10C DeviceNet nel software RSNetWorx avvengono le seguenti modifiche.

Modifiche della configurazione dello scanner RN10C DeviceNet



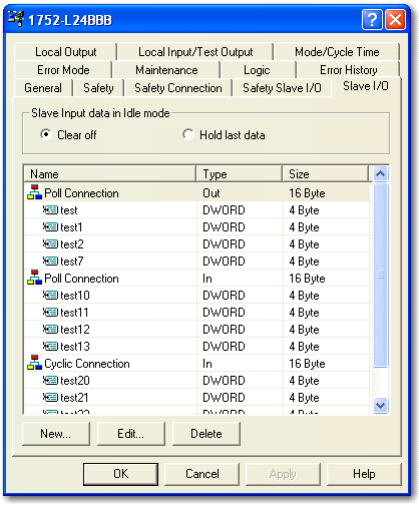


Dimensioni massime della connessione

Questo esempio prevede una connessione di polling con 16 byte in ingresso e 16 byte in uscita. Una seconda connessione (ciclica) di ingresso con 16 byte è stata aggiunta. Quanto segue mostra le modifiche necessarie a supportare la configurazione.

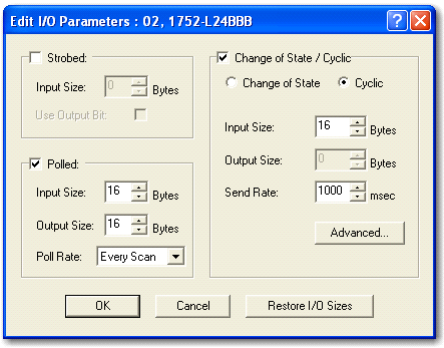
La configurazione I/O dello slave SmartGuard appare come segue.

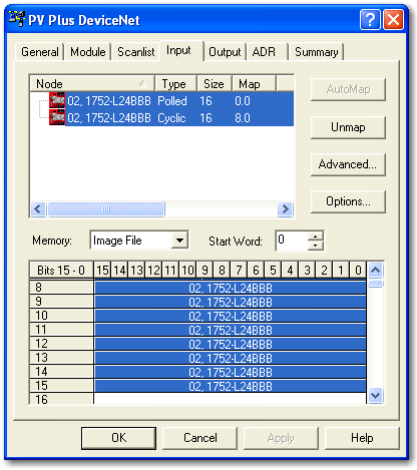
Configurazione I/O dello slave SmartGuard

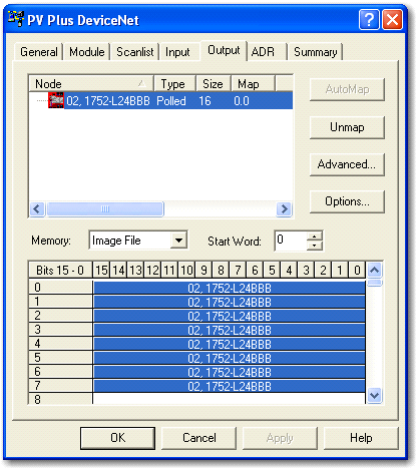


Le proprietà della connessione dello scanner DeviceNet appaiono come illustrato.

Configurazione dello scanner DeviceNet

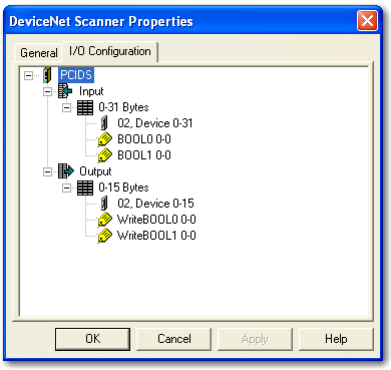






La configurazione I/O del software FactoryTalk to RSView Enterprise appare come illustrato.

Configurazione I/O del software FactoryTalk to RSView Enterprise



Configurazione del controllore per le comunicazioni EtherNet/IP

Introduzione

Il controllore SmartGuard (numero di catalogo 1752-L24BBBE) dispone di connettività EtherNet/IP.

Argomento	Pagina
Configurazione I/O target nel software RSNetWorx for DeviceNet	128
Configurazione del controllore come slave mediante il profilo generico del software RSLogix 5000	132
Configurazione della comunicazione tra un terminale PanelView standard ed un controllore SmartGuard 600 su una rete EtherNet/IP	134

Collegamenti multicast

Il controllore SmartGuard accetta solo due connessioni alla volta. Possono essere un ingresso ed un'uscita o due ingressi o due uscite. Anche se le connessioni sono multicast, una volta fatte le due connessioni, nessuna altra connessione viene accettata.

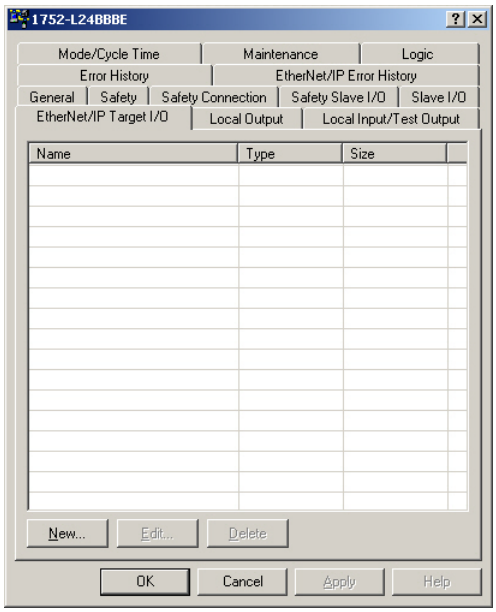
Ad esempio, è possibile avere due controllori collegati ad una connessione di ingresso sul sistema di ingresso multicast del controllore SmartGuard e questo esaurirebbe le due connessioni EtherNet/IP.

Configurazione I/O target nel software RSNetWorx for DeviceNet

Attenersi alla seguente procedura per creare sistemi I/O target EtherNet/IP.

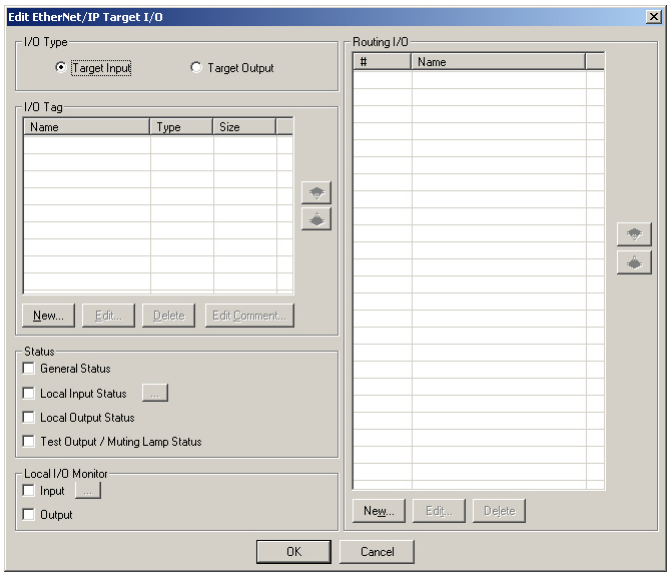
1. Nel software RSNetWorx for DeviceNet, fare clic con il pulsante destro del mouse sul controllore SmartGuard e scegliere Properties.

2. Fare clic sulla scheda EtherNet/IP Target I/O.



3. Fare clic su New.

   Viene visualizzata la seguente finestra di dialogo.



4. In "I/O type", fare clic su Target Input o Target Output.

   Target Input significa che questi dati vengono prodotti dal controllore SmartGuard e letti dal dispositivo origine. Target Output significa che questi dati vengono prodotti dal dispositivo origine ed inviati al controllore SmartGuard.

   Se si seleziona Target Input, è possibile includere le seguenti informazioni di stato nel sistema I/O.

Nome del tag	Dimensione dati	Tipo di attributo
General Status	Byte	Non di sicurezza
Stato degli ingressi locali	Parola	
Stato delle uscite locali	Byte	
Stato dell'uscita di test o della lampada di muting		

5. Aggiungere le informazioni di stato per i tipi di ingresso selezionando le caselle di controllo Status.

6. Aggiungere dati di controllo I/O locale per i vari tipi di ingresso selezionando la casella di controllo Local I/O Monitor appropriata.

Nome del tag	Dimensione dati	Tipo di attributo
Local Input Monitor 1 (ingressi 0...7)	Byte	Non di sicurezza
Local Input Monitor 2 (ingressi 8...15)		
Local Output Monitor (uscite 0...7)		

   I vari tipi di uscita non possono includere dati di controllo I/O locale. È possibile solo leggere i valori di ingresso e di uscita, ma non è possibile sovrascriverli direttamente.

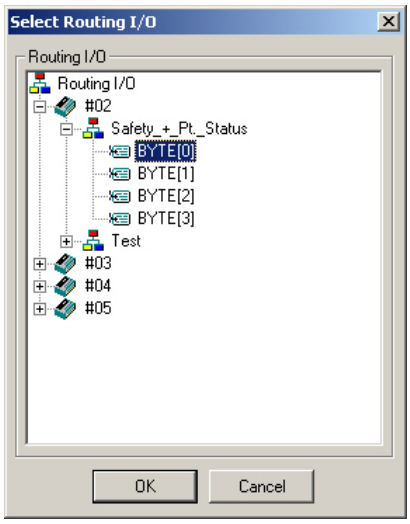
7. Aggiungere i dati Routing I/O per i moduli.

   Se il controllore SmartGuard controlla moduli DIO di sicurezza sulla rete DeviceNet, l'utilizzo della funzione Routing I/O permette di passare i valori dei punti I/O sui moduli DIO ad un controllore standard o ad un'interfaccia operatore sulla rete EtherNet/IP.

   SUGGERIMENTO I moduli appaiono nella tabella Routing I/O solo dopo essere stati aggiunti alla Safety Scan list e dopo aver fatto clic su Apply.

   a. Sotto Routing I/O, fare clic su New.
   b. Espandere il nodo per cui si desidera aggiungere i dati di indirizzamento.
   c. Espandere uno dei sistemi elencati.

d. Selezionare il byte che si desidera aggiungere.



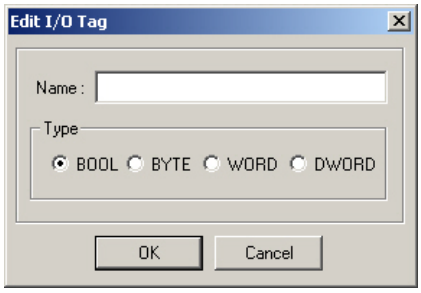
e. Fare clic su OK.

f. Ripetere i passi a...e per aggiungere Routing I/O aggiuntivi.

8. Sotto I/O Tag, fare clic su New per creare un tag I/O.

È possibile definire più tag I/O in un sistema I/O. È possibile definire tag I/O per un massimo di 16 byte in ogni sistema I/O. I tag I/O definiti in questa fase possono essere utilizzati in Logic Editor. Ad esempio, è possibile creare tag che rappresentano errori dalle istruzioni nel codice dei blocchi funzione, per poi visualizzarli su un dispositivo di interfaccia operatore.

Viene visualizzata la seguente finestra di dialogo.

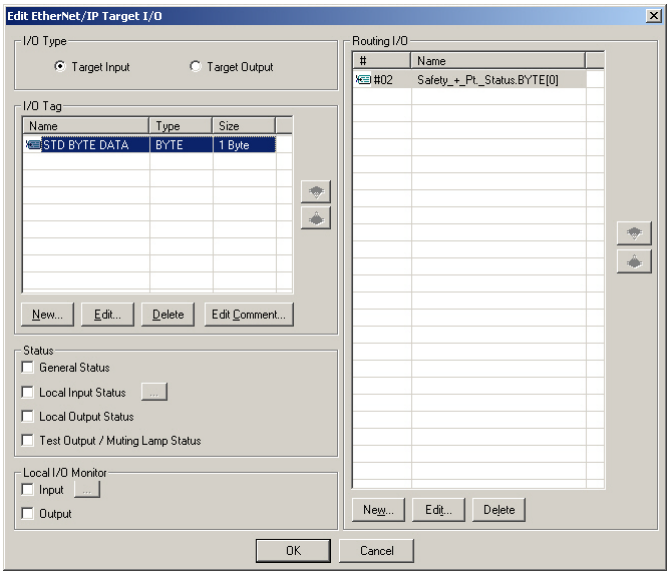


9. Immettere un nome per il tag e selezionare il tipo.

Le opzioni sono BOOL, BYTE, WORD o DWORD.

10. Fare clic su OK.

Viene visualizzata la seguente finestra di dialogo.



11. Creare un nome di tag per ogni bit in un sistema I/O.

a. Sotto I/O Tag, selezionare il sistema desiderato e fare clic su Edit Comment.

b. Immettere un commento per ogni bit nel tag.

I commenti immessi sul nome di tag vengono visualizzati in Logic Editor.

c. Fare clic su OK.

12. Fare clic su OK per tornare alla scheda EtherNet/IP Target I/O.

È possibile creare altri sistemi di ingresso o di uscita, se richiesti nell'applicazione, ripetendo i punti 2...11.

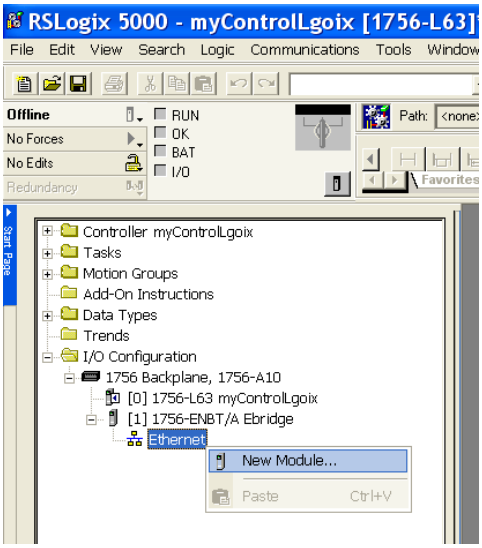
13. Per salvare la configurazione, dal menu File, selezionare Save.

Configurazione del controllore come slave mediante il profilo generico del software RSLogix 5000

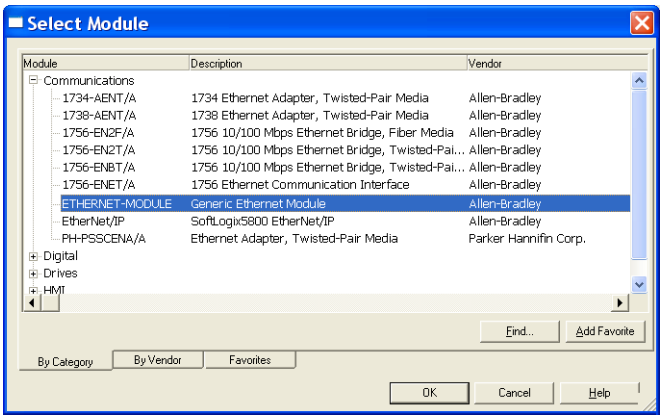
Una volta configurati i dati da condividere nel controllore SmartGuard, è possibile usare il software RSLogix 5000 ed il profilo generico standard per scambiare quei dati con un controllore Logix.

Attenersi alla seguente procedura per effettuare il collegamento al controllore.

1. Fare clic con il pulsante destro del mouse sulla rete Ethernet nell'organizer del controllore e selezionare New Module.



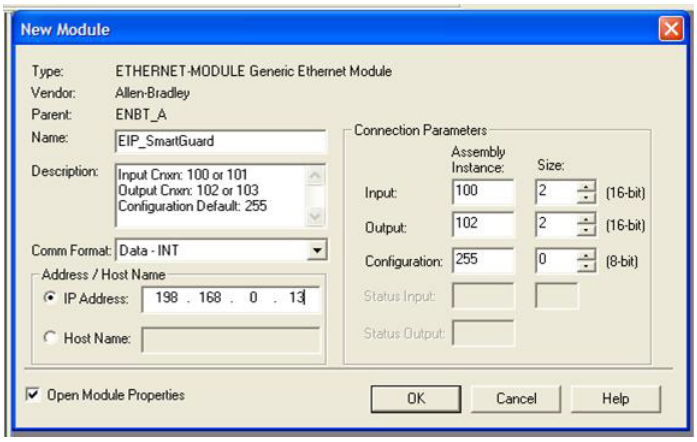
2. Espandere il gruppo Communications e selezionare ETHERNET-MODULE.



3. Fare clic su OK.

4. Nella finestra di dialogo New Module, impostare i parametri come necessario.

Questa finestra di dialogo mostra i valori di istanza per una connessione di ingresso/uscita.



La tabella fornisce i valori di istanza per una connessione di ingresso/uscita ed una connessione di solo ingresso.

Tipo di connessione		Numero istanza
Ingresso/uscita	Ingresso (da controllore SmartGuard a controllore)	100, 101
	Uscita (da controllore a controllore SmartGuard)	102, 103
Solo ingresso	Ingresso	100, 101
	Uscita	199

5. Fare clic su OK.

Configurazione della comunicazione tra un terminale PanelView standard ed un controllore SmartGuard 600 su una rete EtherNet/IP

Per configurare un terminale PanelView standard in modo che possa comunicare con un controllore SmartGuard 600 su un rete EtherNet/IP, procedere come segue.

1. Aprire l'applicazione PanelView nel software PanelBuilder32.

   È necessario definire il percorso di comunicazione tra il terminale PanelView ed il controllore SmartGuard 600.

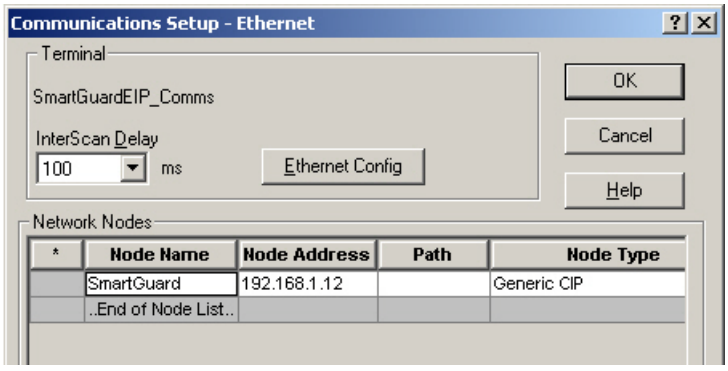
2. Fare clic su Communications Setup.

   Viene visualizzata la finestra di dialogo Communications Setup – Ethernet.

3. Fare clic su Insert.

4. Inserire il nome e l'indirizzo del nodo del controllore SmartGuard.

5. Inserire il tipo di nodo come Generic CIP.



6. Fare clic su OK.

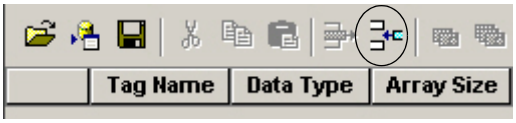
Per definire i tag nel database dei tag di PanelView che accederà ai sistemi I/O target nel controllore SmartGuard 600, procedere come segue.

1. Fare clic su Tag Editor nel menu dell'applicazione.

   Si apre l'editor di tag dell'applicazione.

2. Nella parte inferiore dell'editor di tag, fare clic sulla scheda ENet-CIP.

3. Fare clic su Insert per aggiungere un nuovo tag.



4. Nelle celle del nuovo tag, digitare il Tag Name, un Data Type ed il Node Name (che corrisponde al nome del nodo definito per il controllore SmartGuard in Communications Setup).

   In questo esempio, come tipo di dati è stato scelto DINT.

	Tag Name	Data Type	Descrip	Node Name
1	SG_InputAssembly	DINT		SmartGuard

Il controllore SmartGuard consente la configurazione di fino a quattro sistemi I/O target (due di ingresso e due di uscita).

Per i sistemi di ingresso, i codici del messaggio CIP includono quanto segue:

- Servizio: 0xE – Get Single Attribute
- Classe: 4
- Istanza: 100 o 101 (ingresso 1 o ingresso 2 rispettivamente)
- Attributo: 3

Per i sistemi di uscita, i codici del messaggio CIP includono quanto segue:

- Servizio: 0x10 – Set Single Attribute
- Classe: 4
- Istanza: 102 o 103 (uscita 1 o uscita 2 rispettivamente)
- Attributo: 3

Questo esempio mostra un codice di messaggio CIP che accede a Input Assembly 1 del controllore SmartGuard.

Il campo Member è sempre definito come 1.

1. Dal menu a discesa Service Code, selezionare il codice di servizio CIP.

2. Digitare i codici di classe, istanza e attributi per il tag, in modo da accedere al corretto sistema I/O target nel controllore SmartGuard.

	Tag Name	Data Type	Descrip	Node Name	Initial Value	Array Size	Service Code	Class	Instance	Attribute	Member	Byte Offset
1	SG_InputAssembly	DINT		SmartGuard	0	0	Get Attribute Single (0xE)	4	100	3	1	0

La dimensione massima di un tag membro singolo definito nel terminale PanelView è un DINT (4 byte). Un sistema I/O target nel controllore SmartGuard può arrivare a 16 byte. Per accedere a tutti i byte nel sistema target, è possibile dover creare fino a 4 tag DINT, dove, per ogni tag, viene definito un Offset per la corrispondenza con i byte target di quel tag.

Impostazione delle modalità del controllore

Introduzione

Argomento	Pagina
Impostazione della modalità di esecuzione automatica (opzionale)	137
Impostazione della modalità di comunicazione stand alone (opzionale)	138
Modifica della modalità del controllore	139

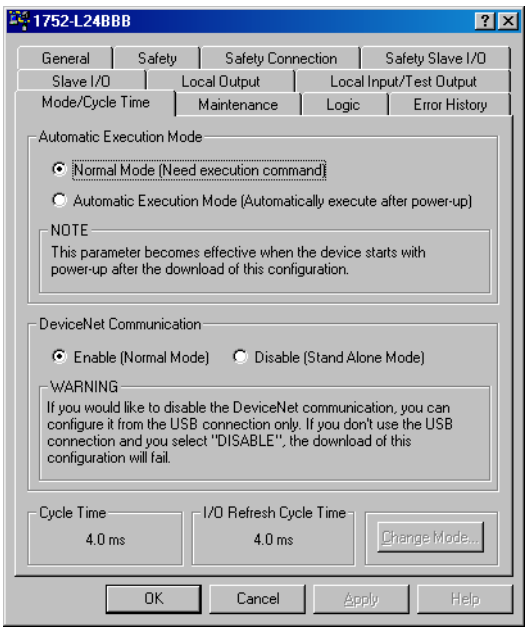
Impostazione della modalità di esecuzione automatica (opzionale)

Il controllore può essere configurato per la modalità normale o la modalità di esecuzione automatica. Impostare la modalità di esecuzione automatica solo dopo aver configurato il sistema. L'impostazione diventa operativa dopo il riavvio in seguito al download di una configurazione.

Attenersi alla procedura seguente per impostare la modalità.

1. Fare clic con il pulsante destro del mouse sul controllore e selezionare Properties.

2. Selezionare la scheda Mode/Cycle Time.



3. Scegliere la modalità normale o di esecuzione automatica.

Modalità	Descrizione
Normal	All'accensione dell'alimentatore, il controllore viene avviato nella modalità di riposo (Idle mode). Utilizzare il software RSNetWorx for DeviceNet per passare alla modalità di esecuzione (Execute mode) facendo clic su Change Mode nella scheda Mode/Cycle Time della finestra di dialogo Controller Properties.
Automatic Execution	All'accensione dell'alimentatore, il controllore viene avviato nella modalità di esecuzione se la configurazione è stata bloccata e il controllore era nella modalità di esecuzione prima dello spegnimento dell'alimentatore.

4. Fare clic su OK.

Impostazione della modalità di comunicazione stand alone (opzionale)

Il controllore SmartGuard può funzionare con o senza le comunicazioni DeviceNet abilitate. L'impostazione di default prevede che le comunicazioni siano abilitate.

Con la modalità Standalone, la durata del ciclo del controllore è più breve, ma le funzioni delle comunicazioni DeviceNet non possono essere utilizzate.

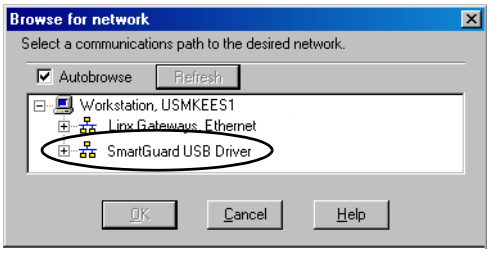
Per utilizzare il controllore SmartGuard nella modalità stand alone, è possibile disabilitare le comunicazioni DeviceNet e utilizzare il collegamento USB per configurare il modulo.

IMPORTANTE Se le comunicazioni DeviceNet vengono disabilitate e non viene utilizzato il collegamento USB, risulterà impossibile scaricare la configurazione.

Attenersi alla procedura seguente per disattivare le comunicazioni DeviceNet.

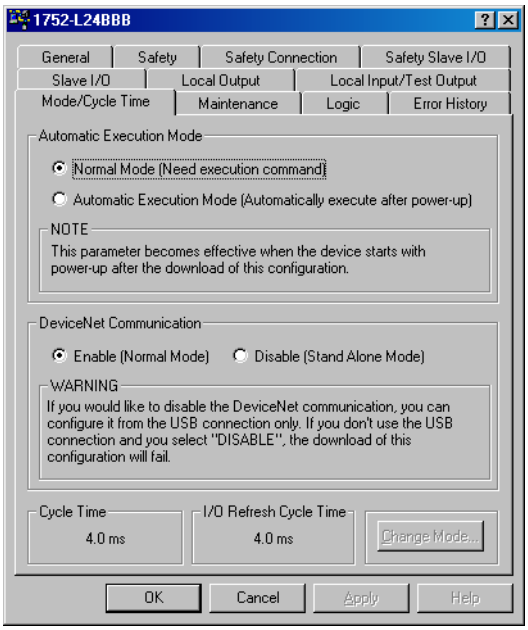
1. Verificare di essere collegati al dispositivo di programmazione tramite il collegamento USB.

2. In caso contrario, impostare un percorso per l'utilizzo del collegamento USB nel software RSNetWorx per DeviceNet.
   a. Dal menu Network, scegliere Properties.
   b. Nella finestra di dialogo DeviceNet, fare clic su Set Online Path.
   c. Nella finestra di dialogo Browse for Network, selezionare il percorso desiderato e fare clic su OK.



3. Nel software RSNetWorx per DeviceNet, fare clic con il pulsante destro del mouse sul controllore e scegliere Properties.

4. Selezionare la scheda Mode/Cycle Time.



5. Scegliere Disable (Stand Alone Mode) e fare clic su OK.

Modifica della modalità del controllore

Attenersi alla seguente procedura per modificare la modalità del controllore.

1. Collegarsi online con il controllore SmartGuard.
2. Fare clic con il pulsante destro del mouse sul controllore e selezionare Properties.
3. Selezionare la scheda Mode/Cycle Time nella finestra di dialogo Controller Properties.
4. Fare clic su Change Mode.
5. Selezionare il pulsante Idle o Execute.
6. Fare clic su OK.

Note:

Creazione di un programma applicativo

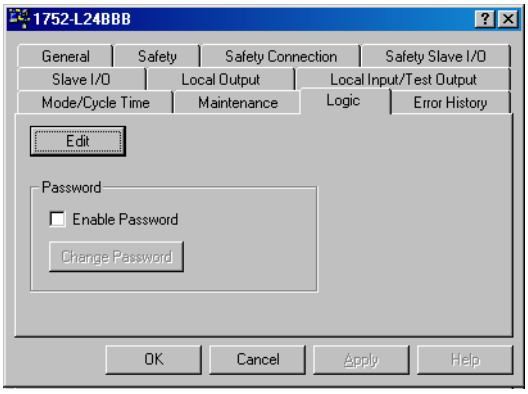
Introduzione

Argomento	Pagina
Logic Editor	141
Principi di programmazione	142
Creazione di un programma con blocchi funzione	147
Modifica dei parametri del blocco funzione	148
Ricerca dei blocchi funzione con collegamenti aperti	151
Programmazione su più pagine	152
Salvataggio del programma	153
Aggiornamento del programma	153
Monitoraggio del programma online	154
Sequenza di esecuzione del programma	155
Blocchi funzione definiti dall'utente	156
Risorse aggiuntive	160

Logic Editor

Il controllore SmartGuard 600 viene programmato con lo strumento Logic Editor del software RSNetWorx for DeviceNet. Logic Editor è costituito da un elenco di oggetti, in cui vengono registrati blocchi funzione, tag I/O e altri elementi di programmazione, e da uno spazio di lavoro, in cui viene eseguita la programmazione.

Per aprire Logic Editor, selezionare la scheda Logic della finestra di dialogo Edit Device Parameters e fare clic su Edit.



È possibile proteggere il programma applicativo con una password per impedirne la modifica, la verifica e la stampa non autorizzate. Per creare una password, attenersi alla procedura seguente.

1. Nella scheda Logic della finestra di dialogo Controller Properties, selezionare la casella di controllo Enable Password.
2. Nella finestra di dialogo Change Password, immettere la password desiderata nel campo New Password.

   Le password possono essere costituite da massimo sei caratteri.
3. Immettere di nuovo la password nel campo Confirm Password.
4. Fare clic su OK.

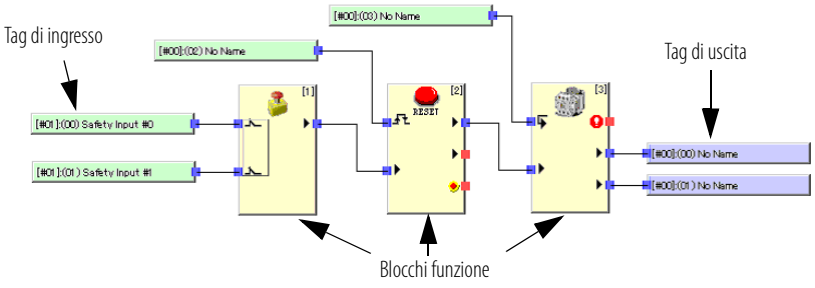
La password verrà richiesta ogni volta che verrà premuto il pulsante Edit per aprire Logic Editor. È possibile caricare o scaricare il programma senza la password, ma le funzioni di modifica, verifica, stampa e report del programma non sono disponibili.

IMPORTANTE Se si dimentica la password, non è possibile recuperarla.

Principi di programmazione

I programmi vengono creati dalle funzioni logiche e dai blocchi funzione che indicano comandi, da tag di ingresso che indicano sorgenti di ingresso dati e da tag di uscita che indicano destinazioni di uscita dati. Gli I/O sono collegati da linee di collegamento.

Collegamenti I/O



Funzioni logiche e blocchi funzione

È possibile utilizzare fino a 254 funzioni logiche e blocchi funzione.

Istruzioni logiche e blocchi funzione supportati

Istruzioni logiche	Blocchi funzione
• NOT • AND • OR • Exclusive OR • Exclusive NOR • Routing • RS Flip-Flop • Multi Connector • Comparator	• Reset • Restart • Emergency stop push-button monitoring • Light curtain monitoring • Safety gate monitoring • Two-hand controller • Off-delay timer • On-delay timer • User Mode Switch • External device monitoring • Muting • Enable switch • Pulse generator • Counter

Tag di ingresso

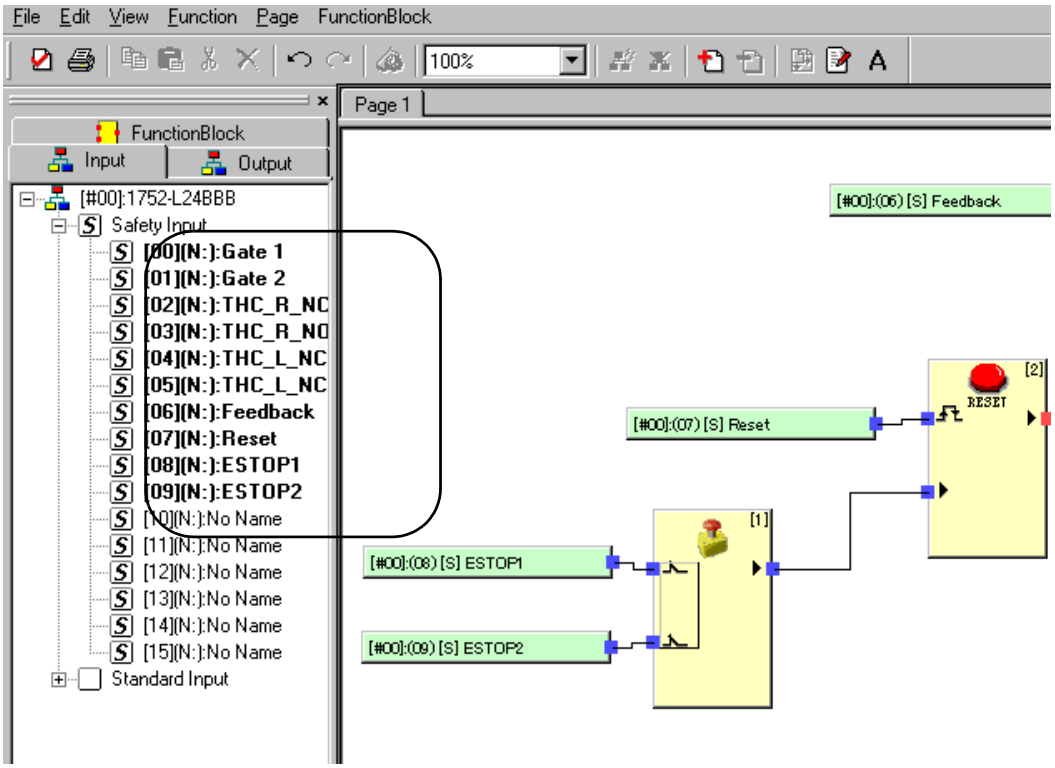
I tag di ingresso riflettono lo stato degli ingressi delle seguenti aree di I/O:

- morsetti locali del controllore
- area di ingresso degli slave di sicurezza registrati come partner di comunicazione
- aree di ingresso riflesse dai dati del master di sicurezza
- aree di ingresso riflesse dai dati del master standard.

I dati sono riflessi nelle seguenti aree di I/O:

- stato degli ingressi locali
- stato delle uscite locali
- stato generale dell'unità
- stato delle uscite di test
- stato della spia di muting.

Nell'elenco degli oggetti, i tag I/O sono visualizzati con dei simboli che indicano il tipo di configurazione.

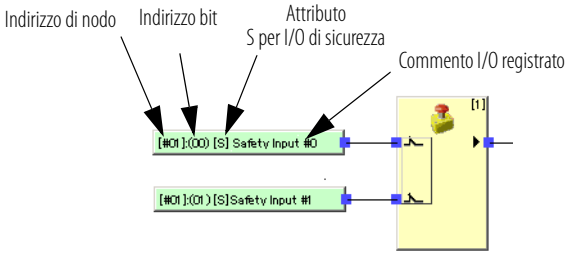


Simboli dei tag di ingresso

Modalità ingresso	Simbolo	Modalità canale	Simbolo
Non utilizzato	N	Singolo	Nessuno
Impulso di test da uscita di test	P	Doppio canale equivalente	e
Utilizzato come ingresso di sicurezza	S	Doppio canale complementare	c
Utilizzato come ingresso standard	ST	–	

Quando vengono utilizzati nello spazio di lavoro, i tag di ingresso includono l'indirizzo di nodo, l'indirizzo bit, l'attributo (S per sicurezza, niente per standard) e il commento I/O registrato.

Tag di ingresso



Tag di uscita

I tag di uscita riflettono lo stato delle uscite delle seguenti aree di I/O:

- morsetti locali del controllore
- area di uscita degli slave di sicurezza registrati come partner di comunicazione
- aree di uscita riflesse dai dati del master di sicurezza
- aree di uscite riflesse dai dati del master standard

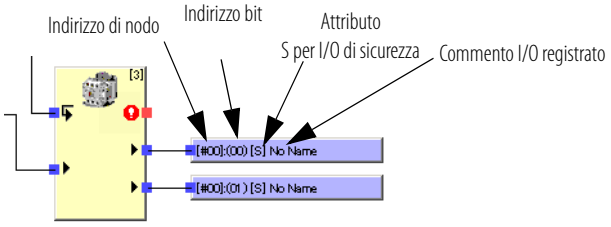
Nell'elenco degli oggetti, i tag I/O sono visualizzati con dei simboli che ne indicano il tipo di configurazione.

Simboli dei tag di uscita

Modalità uscita	Simbolo	Modalità canale	Simbolo
Non utilizzato	N	Singolo	Nessuno
Sicurezza	S	Doppio	d
Test a impulsi di sicurezza	P	–	

Quando vengono utilizzati nello spazio di lavoro, i tag di uscita includono l'indirizzo di nodo, l'indirizzo bit, l'attributo (S per sicurezza, niente per standard) e il commento I/O registrato.

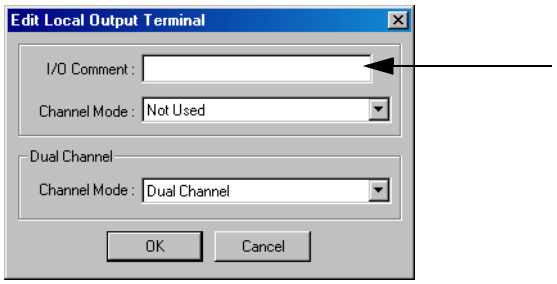
Tag di uscita



Funzione dei commenti I/O

Il commento I/O è un nome opzionale costituito da massimo 32 caratteri ASCII che può essere registrato nel controllore per ogni morsetto I/O utilizzando il software RSNetWorx for DeviceNet. I commenti I/O possono essere utilizzati nell'elenco degli oggetti di Logic Editor come tag I/O, semplificando la programmazione.

Commento I/O



Limitazioni di programmazione

È possibile utilizzare elementi, quali tag I/O e blocchi funzione, in ogni pagina con le seguenti limitazioni:

- Lo stesso tag di ingresso può essere inserito in più pagine.
- Lo stesso tag di ingresso può essere utilizzato una sola volta in ogni pagina.
- Ogni tag di uscita può essere utilizzato una sola volta nel programma applicativo.
- È possibile copiare solo i blocchi funzione. Non è possibile copiare tag I/O, collegamenti di tag I/O e collegamenti tra blocchi funzione.
- Quando un blocco funzione viene incollato, viene inserito nella stessa posizione del blocco funzione da cui è stato copiato. Quando viene incollato un blocco funzione nella stessa pagina, spostare il blocco funzione di origine.
- È possibile utilizzare massimo 254 blocchi funzione.
- È possibile utilizzare massimo 128 indirizzi di salto.
- È possibile utilizzare massimo 32 pagine.
- È possibile utilizzare massimo 128 caselle di testo per i commenti del programma.
- Non è possibile modificare l'impostazione della pagina se sono presenti elementi nello spazio di lavoro. Impostare prima le dimensioni dello spazio di lavoro selezionando File>Page Setup.

Creazione di un programma con blocchi funzione

Per creare un programma con blocchi funzione, creare i collegamenti dal blocco funzione ai tag di ingresso e uscita.

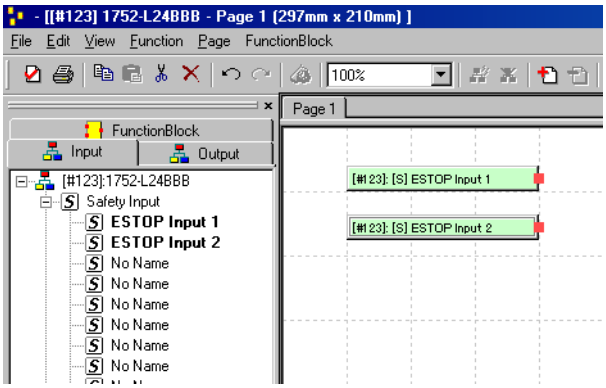
Aggiunta di un tag di ingresso o uscita

Per aggiungere un tag, attenersi alla procedura seguente.

1. Fare clic sulla scheda Input o Output nell'elenco degli oggetti.
2. Selezionare il tag da utilizzare e trascinarlo nello spazio di lavoro.

   È possibile selezionare più tag I/O e aggiungerli contemporaneamente.

Inserimento di tag di ingresso



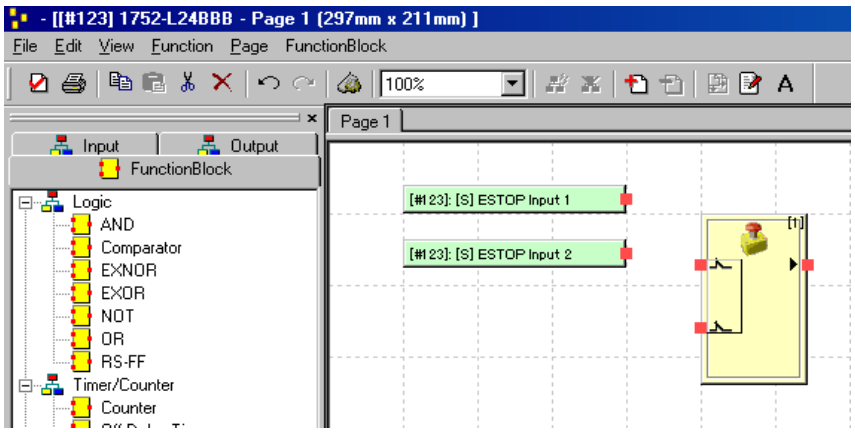
SUGGERIMENTO I tag di ingresso e uscita utilizzati nel programma applicativo vengono visualizzati in grassetto nell'elenco degli oggetti.

Aggiunta di un blocco funzione

Per aggiungere un blocco funzione nello spazio di lavoro, attenersi alla procedura seguente.

1. Fare clic sulla scheda Function Block nell'elenco degli oggetti.
2. Selezionare il blocco funzione da utilizzare e trascinarlo nello spazio di lavoro.

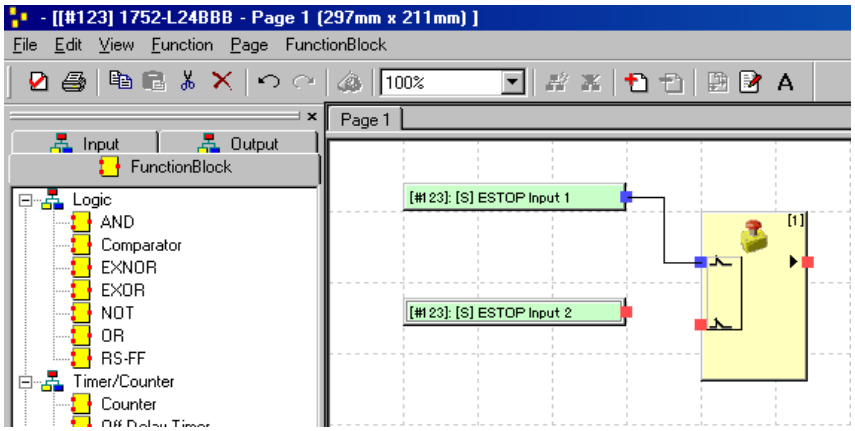
Inserimento di un blocco funzione



Collegamento dei tag al blocco funzione

Per collegare i tag I/O al blocco funzione, fare clic sul connettore di origine (■) e trascinarlo nel connettore di destinazione (■).

Collegamento dei tag ai blocchi funzione

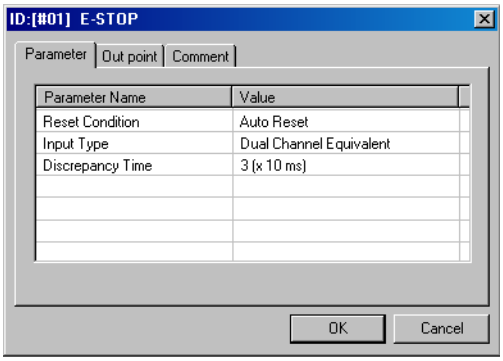


Modifica dei parametri del blocco funzione

È possibile modificare i blocchi funzione cambiando le impostazioni dei parametri e il numero degli ingressi o delle uscite oppure aggiungendo I/O opzionali e commenti relativi all'applicazione. I parametri modificabili variano a seconda del tipo di blocco funzione.

Per aprire la finestra di dialogo Function Block Properties, fare clic con il pulsante destro del mouse sul blocco funzione e selezionare Edit.

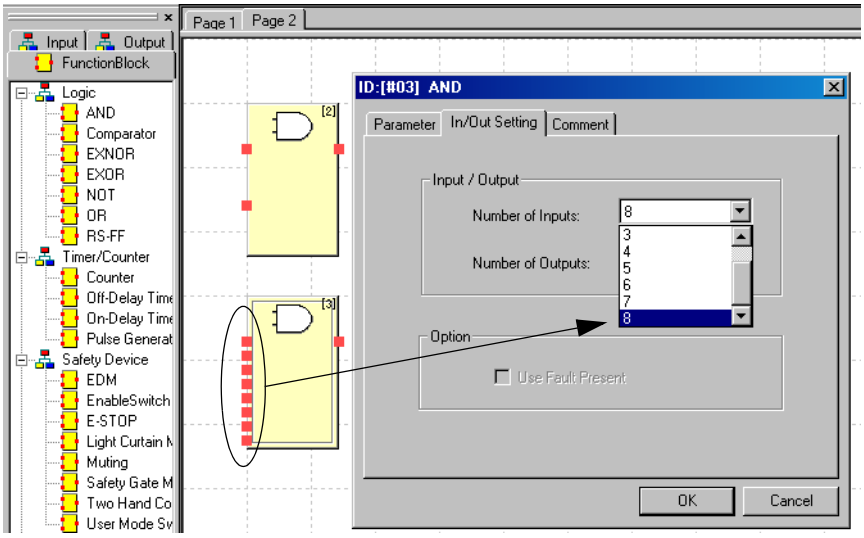
Scheda Parameter



Impostazioni degli ingressi o delle uscite

È possibile modificare le impostazioni Number of Inputs, Number of Outputs e, in alcuni casi, Fault Present di numerose istruzioni.

Scheda In/Out Setting



Number of Inputs

È possibile aumentare il numero di ingressi per le funzioni logiche o abilitare l'ingresso opzionale per i blocchi funzione.

Number of Outputs

È possibile aumentare il numero di uscite per le funzioni logiche o abilitare le uscite opzionali, ad esempio le uscite di errore, dei blocchi funzione.

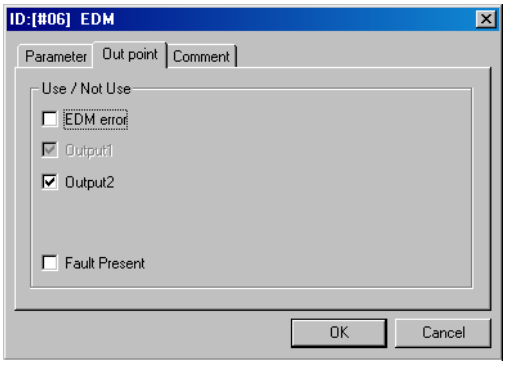
Fault Present Bit

È possibile abilitare il bit di stato diagnostico di presenza guasto in alcuni blocchi funzione selezionando la relativa casella di controllo nella scheda In/Out Setting della finestra di dialogo Function Block Properties. Se la casella di controllo Use Fault Present è selezionata, nel blocco funzione viene visualizzata un'uscita aggiuntiva di presenza guasto.

Selezione di punti di uscita opzionali

È possibile abilitare uscite opzionali, incluso il bit di presenza guasto per alcuni blocchi funzione, selezionando le caselle di controllo opportune nella scheda Out point della finestra di dialogo Function Block Properties. Se le uscite opzionali sono selezionate, vengono visualizzate nel blocco funzione.

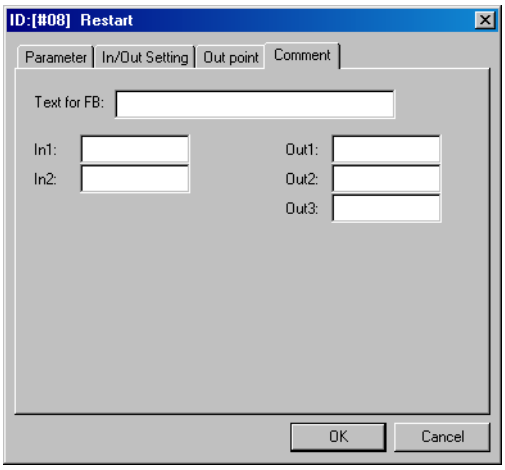
Scheda Out point



Commenti

Selezionare la scheda Comment per specificare un nome per il blocco funzione o i segnali I/O. I nomi dei segnali I/O non vengono visualizzati nello spazio di lavoro, mentre il nome del blocco funzione viene visualizzato sotto il blocco funzione nello spazio di lavoro. Tutti i nomi immessi in questa finestra di dialogo vengono stampati quando viene eseguita la stampa del programma applicativo.

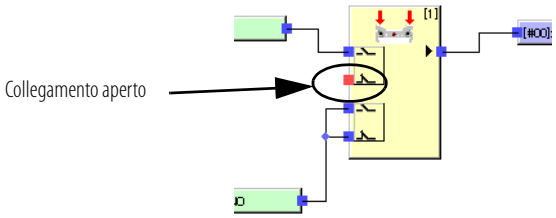
Scheda Comment



Ricerca dei blocchi funzione con collegamenti aperti

Non è possibile scaricare programmi appena creati che contengono blocchi funzione con uscite o ingressi aperti. Devono essere utilizzati tutti gli I/O.

Blocco funzione con collegamenti aperti



Per individuare tutti i collegamenti aperti in Logic Editor, selezionare Edit>Search OpenConnection.

Nella finestra di dialogo Open Connection vengono visualizzati tutti i blocchi funzione con collegamenti aperti. Fare doppio clic su un elemento dell'elenco per visualizzare il blocco funzione. I collegamenti aperti vengono visualizzati in rosso nello spazio di lavoro.

SUGGERIMENTO

Se per il punto di I/O viene utilizzato un indirizzo di salto e l'indirizzo di salto corrispondente non viene utilizzato, il punto di I/O non verrà visualizzato in rosso e verrà indicato come collegato.

Per informazioni sugli indirizzi di salto, vedere Programmazione su più pagine a pagina 152.

Programmazione su più pagine

Il controllore SmartGuard 600 supporta fino a 32 pagine di logica di programmazione.

Per creare una nuova pagina, fare clic sull'icona Add Page .

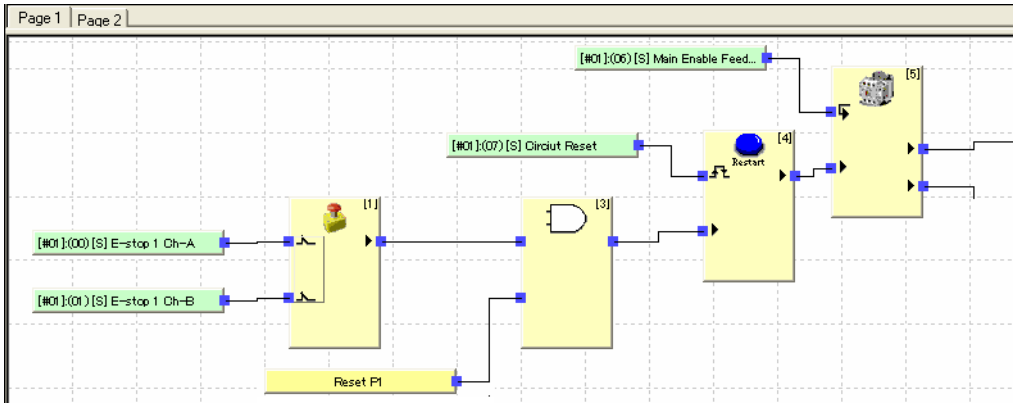
Utilizzare gli indirizzi di salto per collegare la logica tra le pagine. Un programma del controllore SmartGuard 600 può contenere fino a 128 indirizzi di salto.

Per creare un indirizzo di salto, attenersi alla procedura seguente.

1. Fare clic con il pulsante destro del mouse su un qualsiasi punto della pagina di programmazione, quindi selezionare Make JumpAddress.

2. Immettere un nome per l'indirizzo di salto.

3. Collegare l'indirizzo di salto al blocco funzione.

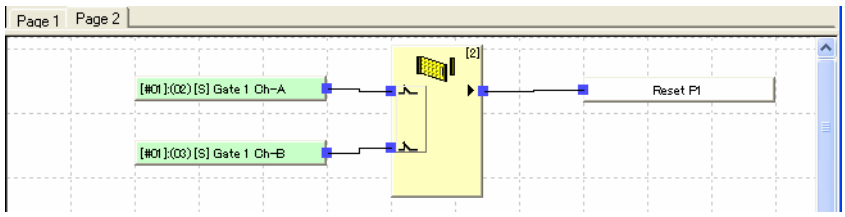


4. Selezionare la pagina a cui collegare la logica.

5. Fare clic con il pulsante destro del mouse su un qualsiasi punto della pagina di programmazione, quindi selezionare Select JumpAddress.

6. Selezionare l'indirizzo di salto dal menu a discesa.

7. Collegare l'indirizzo di salto al blocco funzione.



Salvataggio del programma

Per salvare il programma applicativo, attenersi alla procedura seguente.

1. Selezionare File>Apply.

   Il programma viene salvato temporaneamente nel software RSNetWorx per DeviceNet.

2. Chiudere Logic Editor selezionando File>Exit.

3. Fare clic su OK o su Apply nella finestra di dialogo Edit Device Parameters.

   Se non si fa clic su OK o su Apply oppure se si fa clic su Cancel, le modifiche apportate al programma non vengono salvate. La programmazione salvata temporaneamente utilizzando File>Apply viene eliminata.

4. Selezionare Save o Save As nella finestra di dialogo principale del software RSNetWorx for DeviceNet.

Aggiornamento del programma

Se i tag I/O degli slave di sicurezza che configurano gli I/O locali del controllore SmartGuard vengono modificati, è necessario avviare Logic Editor e verificare il programma.

Se i parametri vengono caricati nel controllore senza avviare Logic Editor, si verifica un errore di download in Logic Editor poiché i dati non corrispondono. In tal caso, avviare Logic Editor e verificare il programma, apportando tutte le modifiche necessarie.

Monitoraggio del programma online

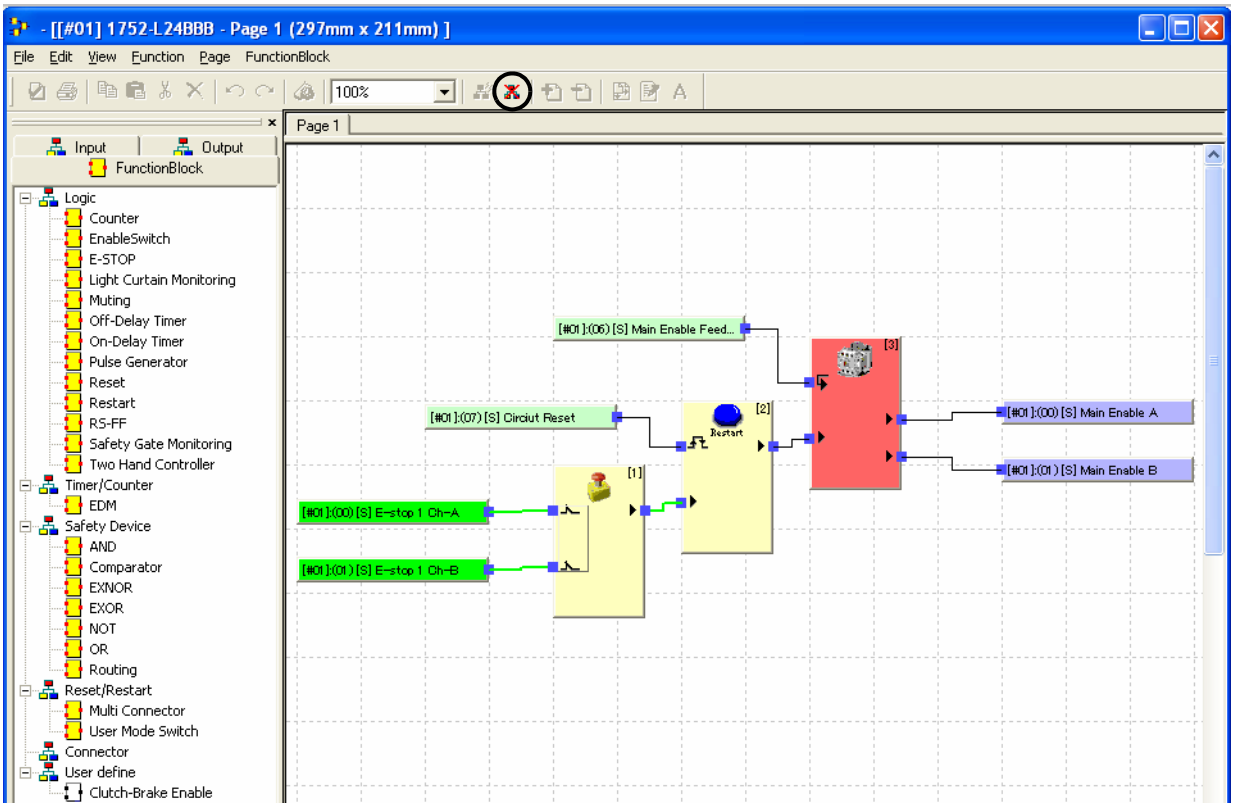
I valori dei tag I/O e gli stati dei segnale dei collegamenti con blocchi funzione possono essere monitorati online in Logic Editor. Accertarsi che il software RSNetWorx per DeviceNet sia collegato alla rete e che il controllore monitorato sia in modalità Run prima di avviare il monitoraggio del programma online.

IMPORTANTE Per il monitoraggio online, potrebbe essere necessario modificare la modalità del controllore impostandola su Execute.

Per avviare il monitoraggio online, fare clic su Monitoring nella barra degli strumenti.

Durante il monitoraggio, i tag I/O o i collegamenti attivi vengono visualizzati con un colore più scuro.

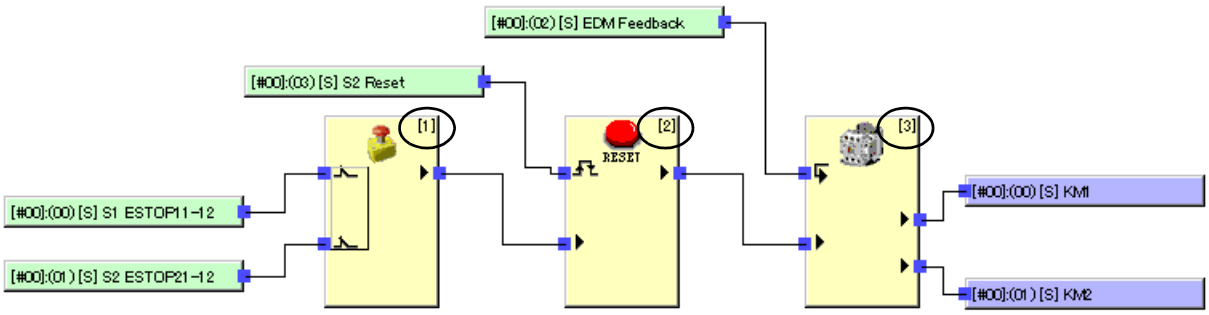
Per interrompere il monitoraggio online, fare clic su Stop Monitoring nella barra degli strumenti.



Sequenza di esecuzione del programma

L'ordine di esecuzione dei blocchi funzione viene impostato automaticamente da Logic Editor e visualizzato nell'angolo destro di ogni blocco funzione.

Programma di esempio

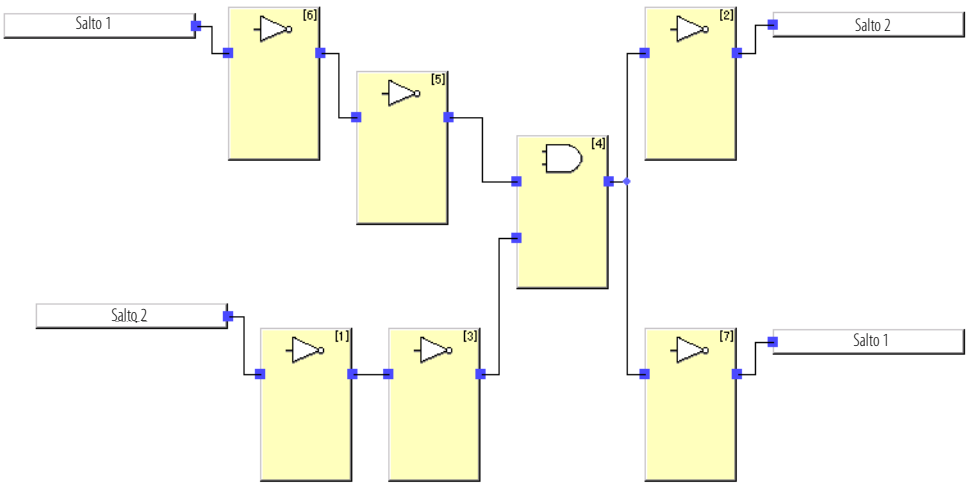


In questo esempio, l'ordine di esecuzione è il seguente:

1. E-stop
2. Ripristino
3. EDM (External Device Monitoring)

Nei programmi è possibile utilizzare indirizzi di salto per creare loopback. Se un programma contiene più loopback, ad esempio un salto 1-salto 1 e un salto 2-salto 2, la sequenza di esecuzione corrisponde all'ordine di posizione dei blocchi funzione. Verificare attentamente tutti i programmi che contengono più loopback per accertarsi che funzionino correttamente.

Esempio di loopback



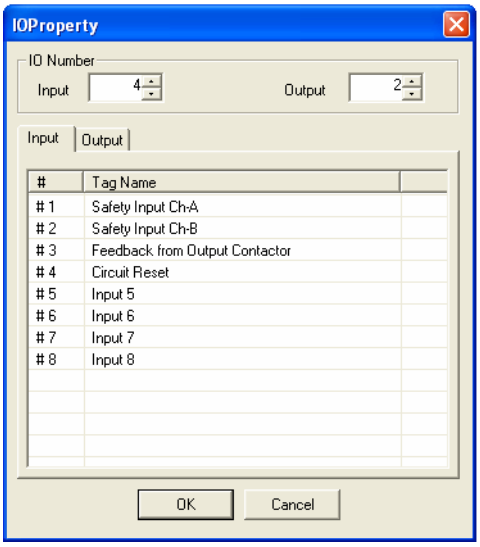
Blocchi funzione definiti dall'utente

Logic Editor consente di creare blocchi funzione definiti dall'utente costituiti dalla logica a blocchi funzione esistente. Una volta creati, questi blocchi funzione vengono memorizzati in una libreria definita dall'utente e possono essere utilizzati in tutte le applicazioni del controllore SmartGuard.

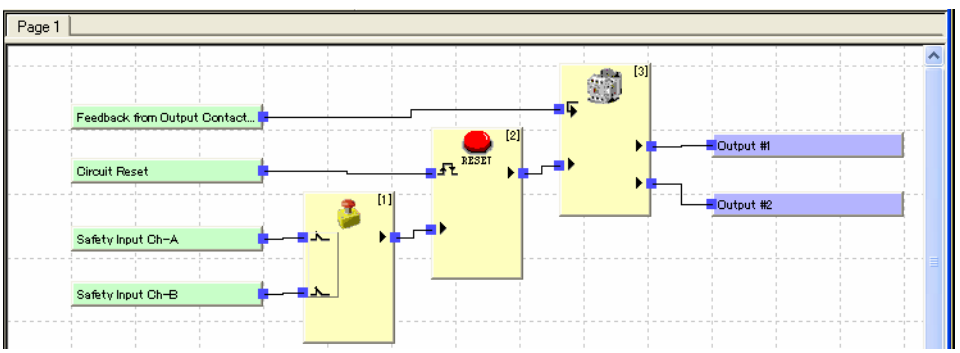
Creazione di blocchi funzione definiti dall'utente

Per creare un blocco funzione definito dall'utente, attenersi alla procedura seguente.

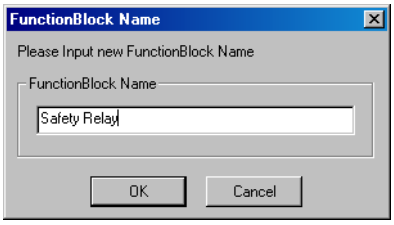
1. Aprire Logic Editor facendo clic con il pulsante destro del mouse sul controllore, selezionando Properties, quindi facendo clic su Edit nella scheda Logic.
2. Selezionare FunctionBlock>Create.
3. Nella finestra di dialogo IOProperty, definire il numero di ingressi e uscite per il blocco funzione.



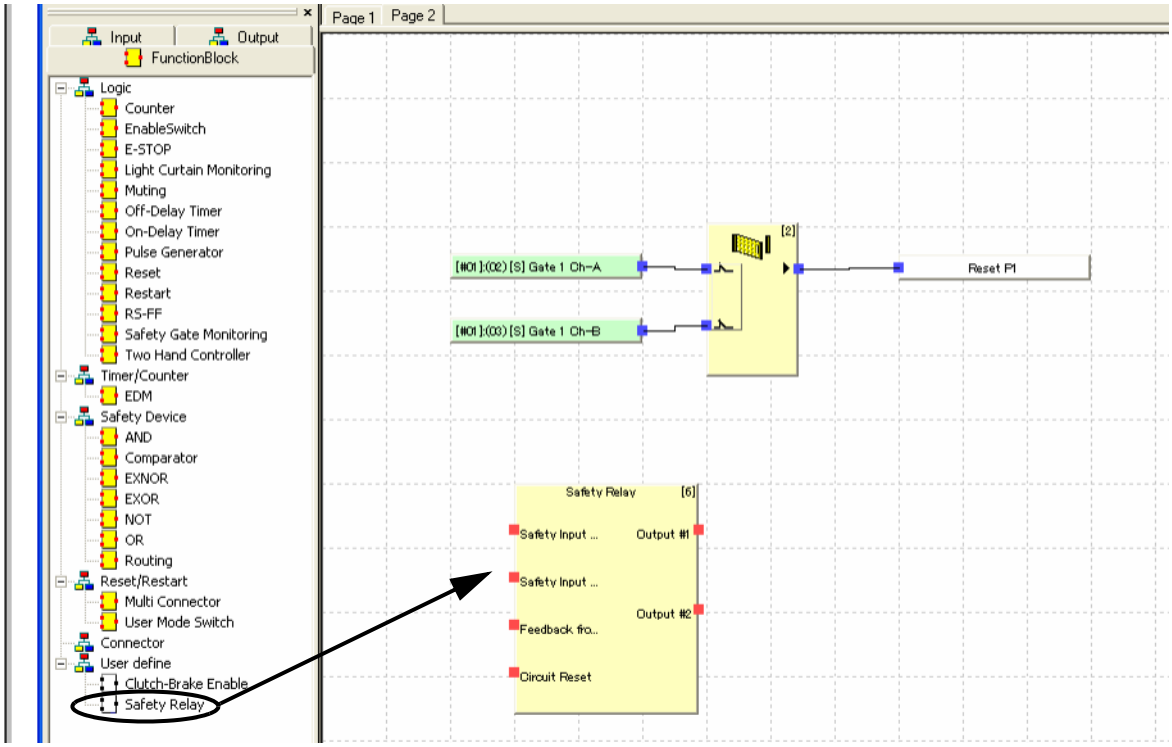
4. Assegnare i nomi a ogni ingresso e uscita.
5. Fare clic su OK per aprire Function Block Logic Editor.
6. Scrivere la logica per il blocco funzione.



7. Selezionare File>Save e immettere un nome per il blocco funzione, quando richiesto.



8. Aggiungere il nuovo blocco funzione alla logica dell'applicazione.



SUGGERIMENTO Se si desidera modificare il blocco funzione definito dall'utente, non è possibile utilizzarlo nell'applicazione corrente. In tal caso, l'opzione di modifica non è disponibile.

IMPORTANTE Scaricare sempre i programmi con i blocchi funzione definiti dall'utente nel controllore, quindi verificarne la configurazione e il funzionamento prima di utilizzarli in un'applicazione.

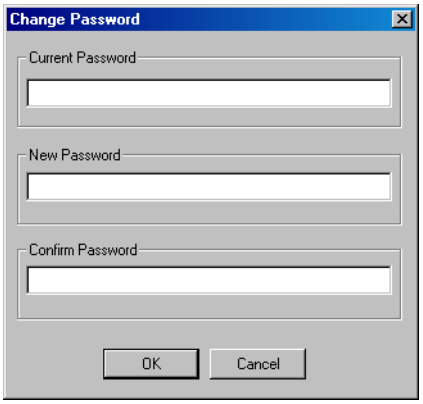
Protezione con password dei blocchi funzione definiti dall'utente

È possibile impostare una password per proteggere i file dei blocchi funzione definiti dall'utente da modifiche non autorizzate. Non è richiesta la password per le operazioni di verifica, report e stampa.

Per impostare una password, attenersi alla procedura seguente.

1. Per aprire Function Block Editor, fare clic con il pulsante destro del mouse su un blocco funzione definito dall'utente e selezionare Edit.

2. In Function Block Editor, selezionare File>Change Password.



3. Immettere una password costituita da massimo sei caratteri alfanumerici nel campo New Password.

4. Immettere di nuovo la password nel campo Confirm Password.

5. Fare clic su OK.

Il blocco funzione definito dall'utente non può essere modificato o eliminato senza l'immissione della password.

Si consiglia di utilizzare una password per proteggere i blocchi funzione definiti dall'utente già verificati per impedire che subiscano modifiche non autorizzate o accidentali dopo essere stati allocati in un programma utente.

Riutilizzo dei file dei blocchi funzione definiti dall'utente

I file di progetto (*.dnt) e i file dei blocchi funzione definiti dall'utente (*.fbd) sono file distinti. È possibile riutilizzare i file dei blocchi funzione definiti dall'utente per la creazione di programmi. Per importare, salvare, eliminare, verificare o modificare i blocchi funzione definiti dall'utente sono richiesti i privilegi di amministratore Windows.

Per riutilizzare i blocchi funzione definiti dall'utente, attenersi alla procedura seguente.

1. Creare il blocco funzione definito dall'utente come descritto a pagina 156.

2. Verificare il funzionamento del blocco funzione definito dall'utente.
   a. Nell'elenco degli oggetti di Logic Editor, fare clic con il pulsante destro del mouse sul nuovo blocco funzione, quindi selezionare Edit.
   b. Revisionare il programma del blocco funzione e correggere eventuali problemi.

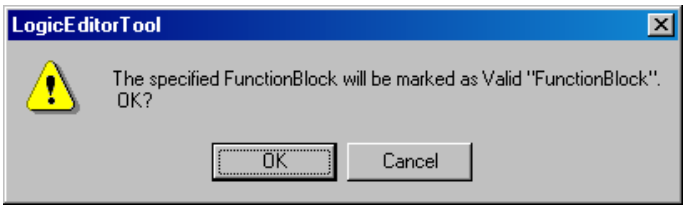
c. Salvare il programma del blocco funzione se sono state apportate modifiche.

d. Chiudere Function Block Logic Editor.

3. Convalidare il blocco funzione definito dall'utente.

a. Nell'elenco degli oggetti di Logic Editor, fare clic con il pulsante destro del mouse sul nuovo blocco funzione, quindi selezionare Validate.

b. Fare clic su OK nella finestra di dialogo di conferma.



L'icona del nuovo blocco funzione cambia da bianco a giallo per indicare che il blocco funzione è stato convalidato.

4. Esportare il blocco funzione definito dall'utente in un file.

a. Nell'elenco degli oggetti di Logic Editor, fare clic sul blocco funzione definito dall'utente salvato.

b. Dal menu principale, selezionare FunctionBlock>Export.

c. Nella finestra di dialogo Save As, immettere un nome per il file, quindi fare clic su Save.

5. Spostare o copiare il file su un altro PC, se necessario.

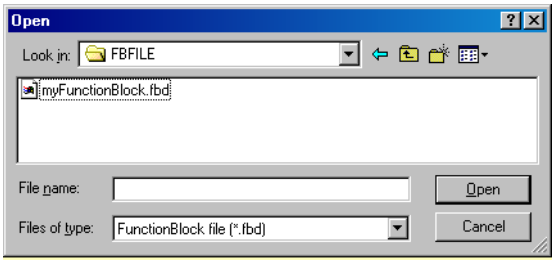
6. Importare il blocco funzione definito dall'utente.

a. Nel software RSNetWorx per DeviceNet, creare un nuovo progetto e aggiungere un controllore SmartGuard.

b. Fare clic con il pulsante destro del mouse sul controllore, scegliere Properties e selezionare la scheda Logic.

c. Fare clic su Edit per avviare Logic Editor.

d. Selezionare FunctionBlock>Import.



e. Selezionare il file appropriato e fare clic su Open.

Nell'elenco degli oggetti di Logic Editor, viene visualizzato il blocco funzione definito dall'utente importato.

IMPORTANTE Importare sempre i file di blocchi funzione definiti dall'utente prima di modificare o verificare i programmi applicativi in cui verranno utilizzati.

Precauzioni per il riutilizzo dei blocchi funzione definiti dall'utente

Nella tabella seguente vengono indicate le azioni che richiedono file dei blocchi funzione definiti dall'utente e viene descritto cosa accade se si tenta di eseguire l'azione senza il file del blocco funzione.

Risultato senza i file dei blocchi funzione

Azione	File	Risultato
Download	Non richiesto	Funziona normalmente
Caricamento	Non richiesto	Funziona normalmente
Salvataggio del file di progetto	Non richiesto	Funziona normalmente
Caricamento del file di progetto	Non richiesto	Funziona normalmente
Verifica	Richiesto	La verifica del programma può essere completata anche senza il file del blocco funzione una volta che il file è stato scaricato nel controllore, ma non è possibile verificare la configurazione del blocco funzione.
Modifica del programma	Richiesto	Viene visualizzato un messaggio di avviso se Logic Editor viene aperto senza il file del blocco funzione. Il blocco funzione definito dall'utente senza un file viene visualizzato con l'icona e tutti i relativi collegamenti vengono eliminati. Le funzioni di modifica, quali copia e incolla, non sono disponibili. Se il programma viene modificato, non è possibile salvarlo o scaricarlo.
Applicazione del programma	Richiesto	Non è possibile eseguire questo comando senza il file del blocco funzione definito dall'utente.

SUGGERIMENTO Se il file del blocco funzione definito dall'utente viene importato con il programma aperto, non viene aggiornato automaticamente. Chiudere e riaprire il programma per visualizzare il blocco funzione correttamente.

IMPORTANTE Verificare sempre il programma originario dopo la modifica dei blocchi funzione definiti dall'utente. Se è stato creato un blocco funzione definito dall'utente, utilizzato poi nel programma originario e modificato dopo il salvataggio del programma, il blocco funzione presente nel programma non viene aggiornato.

Risorse aggiuntive

Risorsa	Descrizione
Appendice C, Riferimento per i comandi delle funzioni logiche	Fornisce informazioni dettagliate sulle funzioni logiche.
Appendice D, Riferimento per i comandi dei blocchi funzione	Fornisce informazioni dettagliate sui blocchi funzione.

Download e verifica

Introduzione

Argomento	Pagina
Download della configurazione di DeviceNet	161
Verifica della configurazione DeviceNet Safety	163
Avvio della procedura guidata Safety Device Verification Wizard	163
Determinazione della possibilità di verificare i dispositivi	164
Selezione dei dispositivi per la verifica	165
Revisione dei report di verifica del dispositivo di sicurezza	167
Blocco di sicurezza dei dispositivi	168
Visualizzazione del riepilogo della procedura guidata Safety Device Verification Wizard	169

Download della configurazione di DeviceNet

Prima di eseguire il download, è necessario collegarsi online alla rete DeviceNet utilizzando il software RSNetWorx for DeviceNet. Il computer e i dispositivi con cui comunicare devono essere collegati alla rete DeviceNet. Se, invece, il controllore è in modalità stand alone, il computer deve essere collegato alla porta USB del controllore SmartGuard.

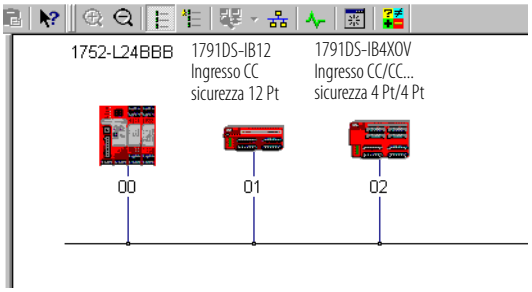
Se si è collegati al controllore SmartGuard con il protocollo EtherNet/IP, è necessario seguire la procedura riportata in questa sezione. Quando si è collegati al controllore SmartGuard mediante il protocollo EtherNet/IP, essenzialmente si crea un ponte, attraverso il controllore SmartGuard, alla rete DeviceNet, per poter andare online, scaricare e monitorare. Anche se questo capitolo tratta il protocollo DeviceNet, la stessa procedura vale per il protocollo EtherNet/IP.

Quando ci si collega online a una rete DeviceNet, il software RSNetWorx per DeviceNet esplora una volta la rete e visualizza i dispositivi di rete rilevati, senza leggere (caricamento) o modificare (download) i parametri dei dispositivi.

La rappresentazione grafica della rete creata dall'operazione di esplorazione è statica, pertanto non viene aggiornata automaticamente per visualizzare le modifiche dall'ultima esplorazione a meno che non sia stata selezionata l'opzione Continuous Browse.

Attenersi alla procedura seguente per scaricare la configurazione di rete DeviceNet.

1. Collegarsi online facendo clic sull'icona online .
2. Selezionare la rete DeviceNet e fare clic su OK quando richiesto.



Durante ogni operazione di esplorazione, il software RSNetWorx per DeviceNet legge i seguenti attributi di ciascun dispositivo.

Attributo di sicurezza	Descrizione
Combinazione del numero della rete di sicurezza (SNN) e dell'indirizzo di nodo	L'indirizzo di nodo e il numero di rete di sicurezza (SNN) memorizzati nel file di configurazione di RSNetWorx per DeviceNet devono corrispondere all'indirizzo di nodo e al numero di rete di sicurezza (SNN) del dispositivo online. Se i numeri di rete di sicurezza (SNN) non corrispondono, viene attivato per il dispositivo lo stato di errore SNN. Per informazioni sulla risoluzione degli errori di mancata corrispondenza dei numeri di rete di sicurezza (SNN), vedere pagina 67.
Autenticazione di configurazione	Il software RSNetWorx per DeviceNet confronta l'autenticazione della configurazione nel file di configurazione con l'autenticazione della configurazione del dispositivo online.
Blocco di sicurezza	Se il dispositivo è in blocco di sicurezza, la configurazione non può essere modificata senza prima sbloccarlo.

3. Scaricare la configurazione sulla rete facendo clic con il pulsante destro del mouse sul dispositivo e selezionando Download to Device.
4. Confermare l'operazione di download facendo clic su Yes.

   Se il dispositivo è protetto da password, il software RSNetWorx per DeviceNet richiede di immettere la password per ogni dispositivo protetto.

   Se il dispositivo è in blocco di sicurezza, è necessario prima sbloccarlo, quindi eseguire il download.

IMPORTANTE Se un dispositivo in blocco di sicurezza viene sbloccato, prima di utilizzarlo in un sistema di sicurezza è necessario eseguire la procedura guidata Safety Device Verification Wizard per verificarlo di nuovo, quindi attivare di nuovo il blocco di sicurezza.

SUGGERIMENTO Se nessun dispositivo è protetto da password o in blocco di sicurezza, è possibile selezionare Download to Network dal menu Network per scaricare la configurazione sulla rete. Tuttavia, questo processo ignora i dispositivi protetti da password o in blocco di sicurezza.

Verifica della configurazione DeviceNet Safety

IMPORTANTE Prima di eseguire la procedura guidata Safety Device Verification Wizard, sfogliare ed esplorare la rete, quindi testare i dispositivi di sicurezza e tutte le relative funzioni di sicurezza di rete per verificarne il corretto funzionamento. È necessario eseguire un test completo dell'applicazione prima di attivare il blocco di sicurezza dei dispositivi.

Per informazioni sul test di verifica delle applicazioni di sicurezza, consultare il Manuale di riferimento per la sicurezza Controllori SmartGuard 600, pubblicazione 1752-RM001.

La procedura Safety Device Verification Wizard, a cui si accede dal software RSNetWorx per DeviceNet, consente di verificare la configurazione dei dispositivi di sicurezza e fornisce gli strumenti per attivare il blocco di sicurezza. Il processo di verifica include il caricamento e il confronto della configurazione memorizzata nel dispositivo e la configurazione memorizzata nel file di configurazione del software RSNetWorx per DeviceNet. La configurazione viene visualizzata in un report per semplificarne la verifica grafica e per consentire futuri riferimenti.

IMPORTANTE Alcuni dispositivi di rete potrebbero non supportare la verifica di Safety Device Verification Wizard. Consultare la documentazione utente per determinare il metodo richiesto per la verifica dei dispositivi.

Avvio della procedura guidata Safety Device Verification Wizard

Attenersi alla seguente procedura per eseguire Safety Device Verification Wizard.

1. Selezionare Network>Safety Device Verification Wizard.

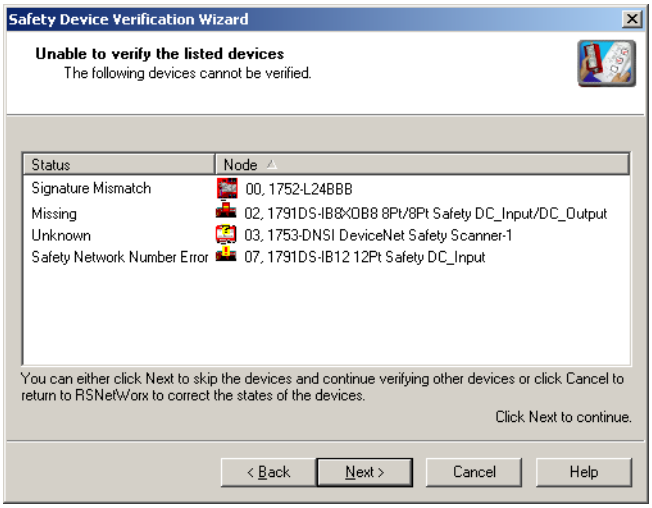
   Viene visualizzata la finestra di dialogo iniziale in cui viene descritto il processo di verifica.

2. Fare clic su Next.

Determinazione della possibilità di verificare i dispositivi

Quando la procedura guidata Safety Device Verification Wizard esplora la rete, controlla lo stato di sicurezza dei dispositivi di rete per determinare se è possibile eseguirne la verifica.

Se alcuni dispositivi sono in uno stato che impedisce il proseguimento del processo di verifica della procedura guidata, viene visualizzata la finestra di dialogo Unable to verify the listed devices in cui sono elencati i dispositivi con i rispettivi stati correnti, oltre a un'icona di stato sovrapposta all'icona del dispositivo.



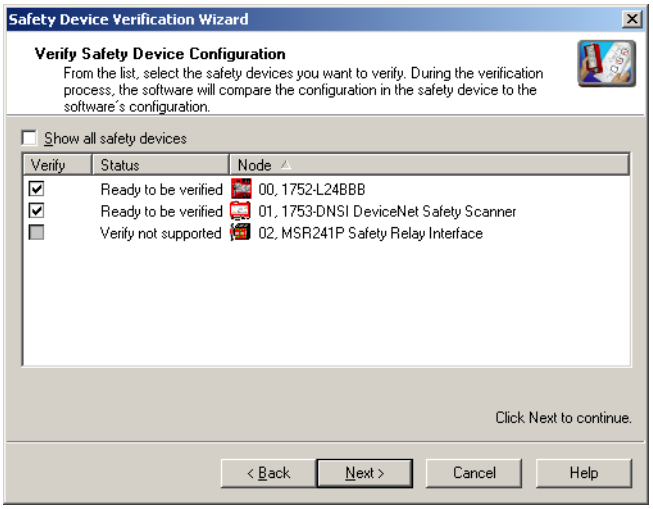
Stato	Icona	Descrizione
Missing		Il dispositivo fa parte della configurazione di rete, ma non è stato trovato durante l'operazione di esplorazione.
Mismatch		L'identità del dispositivo nella configurazione di rete non corrisponde all'identità del dispositivo online.
Unknown		Il dispositivo fa parte della configurazione, ma non è stato ancora rilevato in rete.
Safety Network Number Error		Il numero della rete di sicurezza (SNN) del dispositivo non è valido oppure non corrisponde al numero SNN specificato per il dispositivo nel file di configurazione di RSNetWorx per DeviceNet.
Signature Mismatch	Nessuna	L'autenticazione della configurazione del dispositivo non corrisponde all'autenticazione della configurazione nel file di configurazione di RSNetWorx per DeviceNet.
Safety Locked		Il dispositivo è già bloccato.

Per tornare al software RSNetWorx per DeviceNet e correggere lo stato dei dispositivi indicati, chiudere la procedura guidata Safety Device Verification Wizard facendo clic su Cancel.

Per ignorare i dispositivi elencati e continuare il processo di verifica degli altri dispositivi di sicurezza di rete, fare clic su Next.

Selezione dei dispositivi per la verifica

Scegliere i dispositivi da verificare utilizzando le caselle di controllo nella colonna Verify della finestra di dialogo Verify Safety Device Configuration. È possibile selezionare solo i dispositivi con stato Ready to be verified.



Se la casella di controllo Show all safety devices è selezionata, nella finestra di dialogo vengono elencati tutti i dispositivi di sicurezza di rete con i rispettivi stati correnti. In caso contrario (impostazione di default), vengono visualizzati solo i dispositivi con gli stati seguenti:

- Verify FAILED

  L'operazione di caricamento e confronto ha rilevato che la configurazione del dispositivo non corrisponde alla configurazione nel file di configurazione di RSNetWorx per DeviceNet.

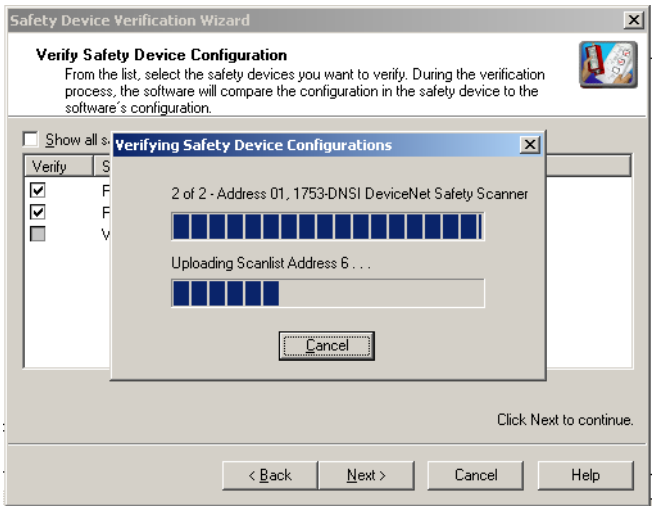
- Ready to be verified

  Il dispositivo non è in blocco di sicurezza e può essere selezionato per la verifica.

- Verify not supported

  Il dispositivo non è in blocco di sicurezza, ma non supporta la verifica tramite la procedura guidata Safety Device Verification Wizard. Consultare la documentazione utente per informazioni sulla modalità di verifica del dispositivo. Dopo la verifica del dispositivo, è possibile attivare il blocco di sicurezza utilizzando la procedura guidata.

Fare clic su Next per avviare il processo di caricamento e confronto.



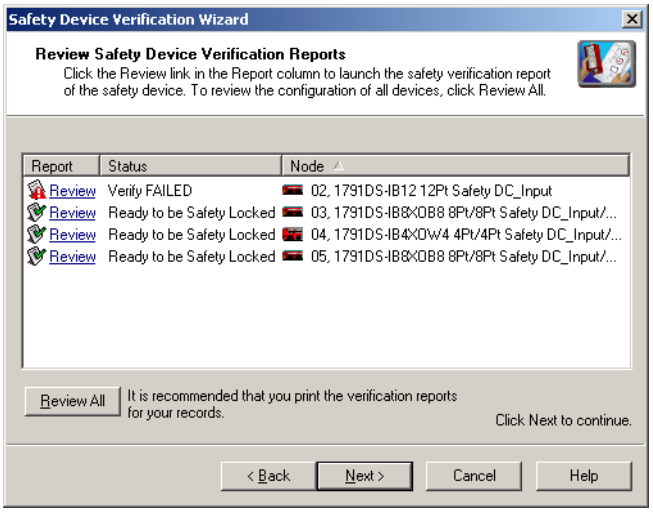
SUGGERIMENTO

Facendo clic su Next senza alcun dispositivo selezionato per la verifica, la procedura guidata controlla se i dispositivi sono stati verificati o se sono pronti per essere bloccati durante l'esecuzione corrente della procedura guidata.

Se	La procedura guidata visualizza
i dispositivi sono stati verificati	la finestra di dialogo Review in cui sono elencati i dispositivi.
i dispositivi sono pronti per l'attivazione del blocco di sicurezza	la finestra di dialogo Lock in cui sono elencati i dispositivi.
non è stato verificato alcun dispositivo	la finestra di dialogo Finish.
nessun dispositivo è pronto per l'attivazione del blocco di sicurezza	la finestra di dialogo Finish.

Revisione dei report di verifica del dispositivo di sicurezza

Nella pagina Review vengono visualizzati i dispositivi di sicurezza con i relativi stati: Verify FAILED o Ready to be Safety Locked.



1. Fare clic su Review nella colonna Report per aprire il report in formato HTML del dispositivo nel browser di default.
2. Fare clic su Review All per generare un report di verifica in formato HTML per tutti i dispositivi elencati.

   SUGGERIMENTO Se lo stato di un dispositivo è Verify FAILED, nel report di errore di verifica vengono fornite ulteriori informazioni.

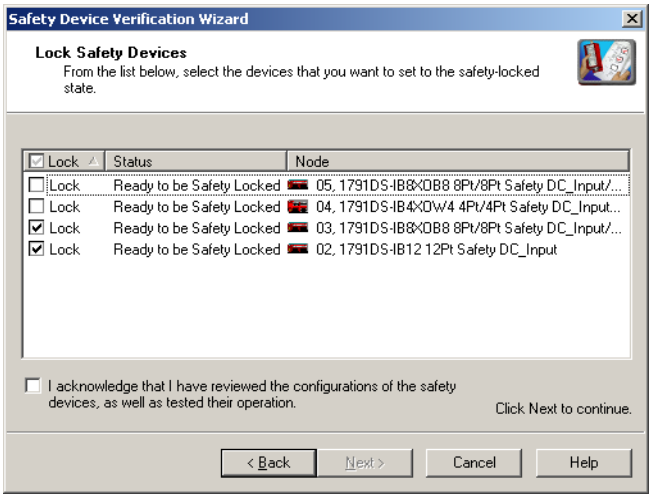
3. Esaminare i report di verifica e stamparli per futuri riferimenti.

IMPORTANTE Verificare le configurazioni dei dispositivi e registrare le autenticazioni di configurazione prima di utilizzare un'applicazione di sicurezza.

Blocco di sicurezza dei dispositivi

IMPORTANTE Prima di bloccare le configurazioni dei dispositivi di sicurezza, è necessario eseguire completamente la procedura di verifica richiesta per l'applicazione utilizzata.

1. Scegliere i dispositivi per cui attivare il blocco di sicurezza selezionando la casella di controllo nella colonna Lock di ogni dispositivo pronto per l'attivazione del blocco di sicurezza.



2. Per poter continuare il processo di blocco, è necessario selezionare la casella di controllo di conferma.

3. Fare clic su Next.

   Prima di bloccare un dispositivo, la procedura guidata esegue un confronto finale tra l'autenticazione della configurazione di ogni dispositivo di sicurezza e la rispettiva autenticazione della configurazione nel software RSNetWorx per DeviceNet.

4. Se alcuni dei dispositivi selezionati sono protetti da password, verrà richiesto di immettere le rispettive password.

   Per ignorare il dispositivo e continuare il processo di blocco per gli altri dispositivi, fare clic su Skip.

Visualizzazione del riepilogo della procedura guidata Safety Device Verification Wizard

Prima di essere chiusa, la procedura guidata visualizza un riepilogo di tutti i dispositivi di sicurezza per cui è stato attivato il blocco di sicurezza, indica il numero di dispositivi di sicurezza per cui deve essere ancora attivato il blocco di sicurezza e consente di visualizzare lo stato, verificato o in blocco di sicurezza, di tutti i dispositivi di sicurezza di rete.

Fare clic su Finish per chiudere la procedura guidata.

Note:

Monitoraggio dello stato e gestione degli errori

Introduzione

Argomento	Pagina
Indicatori di stato	171
Display alfanumerico	172
Monitoraggio dell'ingresso di alimentazione I/O	173
Monitoraggio delle informazioni sulla manutenzione I/O	174
Visualizzazione dei dati di stato I/O	177
Stato di collegamento del controllore (funzione di slave di sicurezza)	180
Categorie di errore	182
Tabella cronologica degli errori	183
Messaggi della cronologia errori e azioni correttive	186
Errori di download e azioni correttive	190
Errori di ripristino e azioni correttive	192
Errori di modifica della modalità e azioni correttive	193

Indicatori di stato

Il controllore SmartGuard 600 è dotato di indicatori di stato per il modulo, le reti DeviceNet e EtherNet/IP, il blocco, la comunicazione USB e EtherNet/IP, gli ingressi e le uscite individuali, oltre che di un display alfanumerico per i codici di errore DeviceNet, l'indirizzo di nodo DeviceNet e le informazioni dell'indirizzo EtherNet/IP.

Per una descrizione delle combinazioni di colore e stato degli indicatori di stato e delle azioni consigliate, vedere l'Appendice B.

Display alfanumerico

Il display alfanumerico del controllore fornisce i codici di errore DeviceNet, l'indirizzo di nodo DeviceNet e le informazioni dell'indirizzo EtherNet/IP. Durante il normale funzionamento, sul display viene visualizzato l'indirizzo di nodo del modulo, da 00 a 63 in formato decimale. Se il controllore funziona in modalità stand alone (non in rete), sul display viene visualizzata l'indicazione "nd". Il display lampeggia durante l'autotest, la configurazione o la modalità di riposo del controllore. In caso di guasti, sul display vengono visualizzati alternativamente il codice di errore e l'indirizzo di nodo in cui si è verificato l'errore. Se si verifica un errore irreversibile, sul display viene visualizzato solo il codice di errore.

Quando l'interruttore di servizio viene premuto, il display mostra l'autenticazione di configurazione di sicurezza del controllore, due cifre alla volta. L'autenticazione di configurazione viene visualizzata anche nella scheda Safety della finestra di dialogo Properties del controllore nel software RSNetWorx for DeviceNet. È possibile utilizzare l'autenticazione di configurazione per verificare che il programma e la configurazione del controllore non siano stati modificati.

Quando il pulsante di visualizzazione dell'indirizzo IP viene premuto per almeno 1 secondo, il display visualizza l'indirizzo EtherNet/IP impostato. Se si verifica un errore nella configurazione EtherNet/IP, viene visualizzato il codice di errore "n4".

Descrizione del funzionamento del display

<table>
<tr><th colspan="2">Stato</th><th colspan="2">Display</th></tr>
<tr><td rowspan="3">Condizioni normali con DeviceNet abilitato</td><td>Modalità operativa: Run Comunicazioni I/O di sicurezza: in funzione</td><td rowspan="3">Viene visualizzato l'indirizzo di nodo del controllore.</td><td>Acceso</td></tr>
<tr><td>Modalità operativa: Run Comunicazioni I/O di sicurezza: non in funzione</td><td>Lampeggiante</td></tr>
<tr><td>Modalità operativa: autotest, configurazione o riposo</td><td>Lampeggiante</td></tr>
<tr><td rowspan="2">Condizioni normali con DeviceNet disabilitato</td><td>Modalità operativa: Run</td><td rowspan="2">Viene visualizzata l'indicazione nd</td><td>Acceso</td></tr>
<tr><td>Modalità operativa: autotest, configurazione o riposo</td><td>Lampeggiante</td></tr>
<tr><td rowspan="3">Condizioni di errore</td><td>Errore grave</td><td>Viene visualizzato solo il codice di errore</td><td>Acceso</td></tr>
<tr><td>Interruzione</td><td>Viene visualizzato solo il codice di errore</td><td>Acceso</td></tr>
<tr><td>Errore reversibile</td><td colspan="2">Vengono visualizzati alternativamente il codice di errore e l'indirizzo di nodo in cui si è verificato l'errore.</td></tr>
</table>

Per una descrizione delle combinazioni di indicatori di stato e codici del display alfanumerico, incluse le azioni correttive, vedere l'Appendice B.

Monitoraggio dell'ingresso di alimentazione I/O

È possibile monitorare l'ingresso di alimentazione I/O utilizzando il display alfanumerico sul pannello frontale del controllore, oltre i dati sullo stato generale delle comunicazioni I/O DeviceNet.

Se un morsetto I/O sul controllore è impostato su un'opzione diversa da Non utilizzato, quando non viene fornita la normale tensione di alimentazione, sul display alfanumerico viene visualizzato:

- P4: l'alimentazione per gli ingressi (V1,G1) non è compresa nell'intervallo consentito.
- P5: l'alimentazione per le uscite (V2,G2) non è compresa nell'intervallo consentito.

Monitoraggio delle informazioni sulla manutenzione I/O

È possibile configurare una modalità di manutenzione e una soglia di allarme per ogni ingresso locale, uscita di test e morsetto di uscita locale utilizzando la scheda Maintenance della finestra di dialogo Controller Properties nel software RSNetWorx for DeviceNet. È possibile configurare un morsetto per il monitoraggio del contatore commutazioni off/on o del tempo totale di funzionamento.

Monitoraggio del contatore commutazioni off/on

Questa funzione di manutenzione conteggia il numero di operazioni 'da off a on' di un morsetto di ingresso locale, di un'uscita di test o di un'uscita locale e lo memorizza internamente nella memoria non volatile.

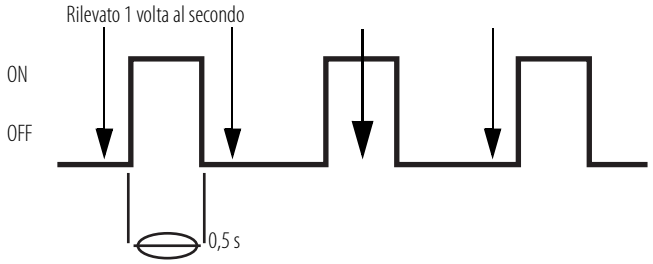
Monitoraggio del tempo totale di funzionamento

Questa funzione di manutenzione tiene traccia del tempo per cui un morsetto di ingresso locale, un'uscita di test o un'uscita locale è attivo e lo memorizza internamente nella memoria non volatile. La funzione di monitoraggio verifica se il dispositivo collegato è attivo ad intervalli di un secondo. Se il dispositivo è attivo per meno di un secondo, il tempo totale di funzionamento potrebbe non essere preciso.

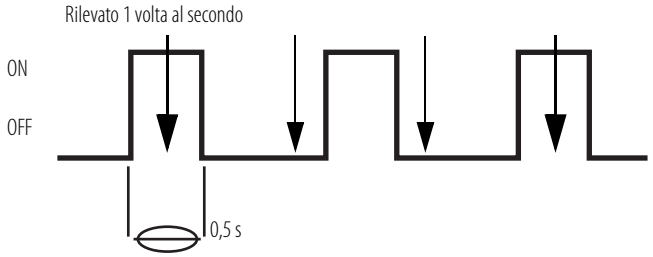
ESEMPIO

Calcolo del tempo totale di funzionamento con impulsi con tempo di on di 0,5 secondi

Nel primo esempio, il bit è effettivamente attivo per 0,5 s x 3 = 1,5 s. Tuttavia, il bit è attivo una sola volta quando viene eseguito il controllo dello stato, quindi il tempo totale di funzionamento rilevato è pari a 1 s.



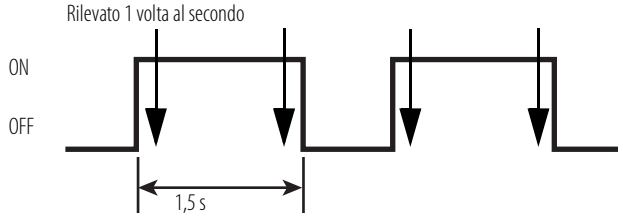
Nel secondo esempio, il bit è effettivamente attivo per 0,5 s x 3 = 1,5 s, ma il bit è attivo per due volte quando viene eseguito il controllo dello stato, quindi il tempo totale di funzionamento rilevato è pari a 2 s.



ESEMPIO

Calcolo del tempo totale di funzionamento con impulsi con tempo di on di 1,5 secondi

Nel seguente esempio, il bit è effettivamente attivo per 1,5 s x 2 = 3 s, ma il bit è attivo per quattro volte quando viene eseguito il controllo dello stato, quindi il tempo totale di funzionamento rilevato è pari a 4 s.

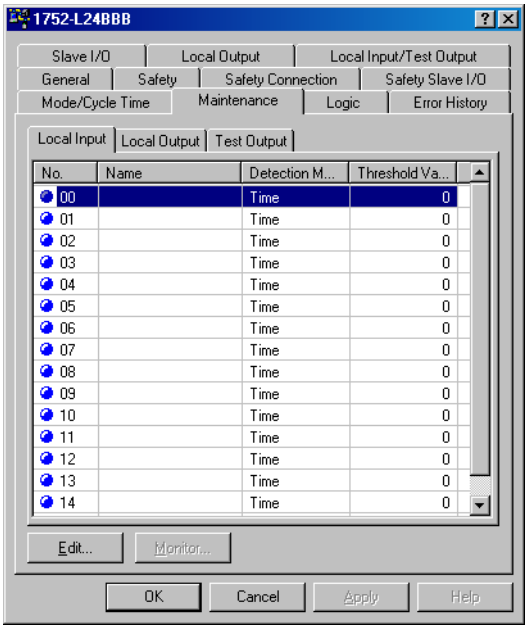


Configurazione di una modalità di monitoraggio di manutenzione

Attenersi alla procedura seguente per configurare la modalità del contatore commutazioni off/on per un morsetto.

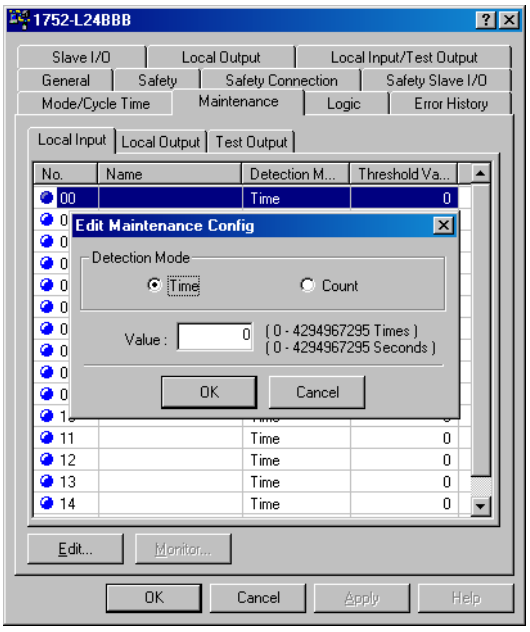
1. Nel software RSNetWorx per DeviceNet, fare clic con il pulsante destro del mouse sul controllore e scegliere Properties.

2. Selezionare la scheda Maintenance.



3. Selezionare la scheda Local Input, Local Output o Test Output.

4. Selezionare il morsetto desiderato e fare clic su Edit.



5. Nella finestra di dialogo Edit Maintenance Config, selezionare la modalità di rilevamento, Count o Time.

6. Immettere un valore di soglia di allarme per la modalità di rilevamento specificata.

Modalità di rilevamento	Intervallo valido per i valori
Time	Da 0 a 4.294.967.295 secondi
Conteggio	Da 0 a 4.294.967.295 volte

7. Fare clic su OK.

8. Fare clic su OK.

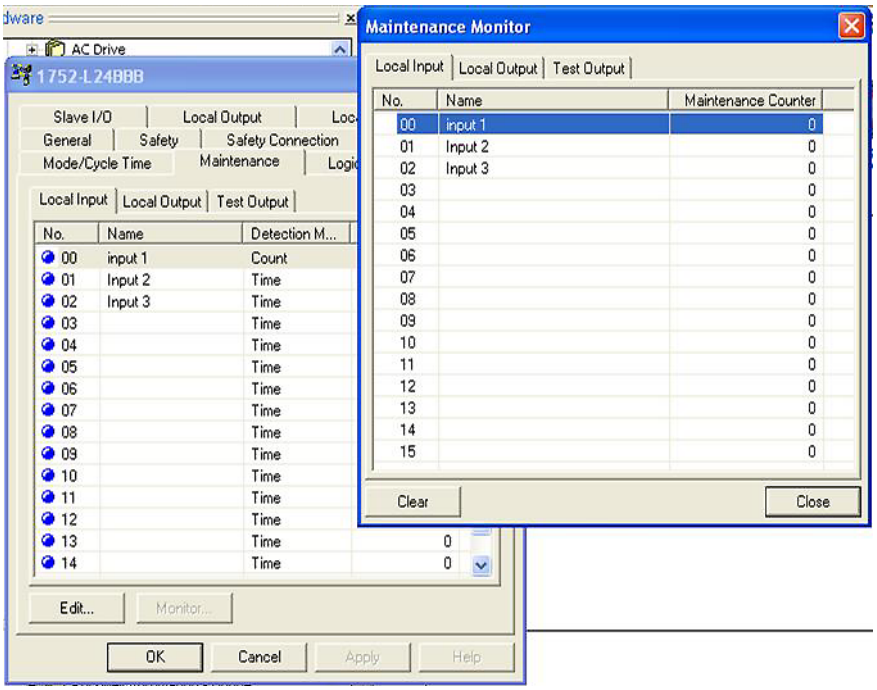
Quando il controllore è online, è possibile monitorare i morsetti configurati facendo clic su Monitor nella scheda Maintenance.

Cancellazione dei valori di manutenzione

Attenersi alla procedura seguente per cancellare i valori accumulati relativi al conteggio o al tempo di funzionamento con il controllore online.

1. Nella scheda Maintenance, fare clic su Monitor.

2. Nella finestra di dialogo Maintenance Monitor fare clic su Clear.



Visualizzazione dei dati di stato I/O

Quando il controllore funge da destinazione di slave di sicurezza o slave standard, è possibile aggiungere le informazioni sullo stato alla prima riga dei dati di trasmissione. Le informazioni possono essere memorizzate in un controllore e utilizzate per realizzare un sistema di monitoraggio.

Dati di stato del controllore

Nome del tag	Dimensione dati	Tipo di attributo
General Status	1 byte	Non di sicurezza
Stato degli ingressi locali	Parola	Sicurezza
Stato delle uscite locali	Byte	Sicurezza
Stato dell'uscita di test o della lampada di muting	Byte	Non di sicurezza

ATTENZIONE

Non utilizzare i dati con un attributo non di sicurezza per configurare il sistema di controllo di sicurezza. Durante la generazione dei dati non di sicurezza non vengono adottate le misure necessarie per i dati di sicurezza.

Dati di stato generale

Gli indicatori di stato generale sono attributi non di sicurezza che indicano lo stato del sistema.

Dettagli sui dati di stato generale

Bit	Nome	Descrizione
0	Indicatore di stato della tensione di alimentazione di ingresso	Indica lo stato della tensione di alimentazione per gli ingressi. OFF: alimentazione normale attiva. ON: errore di tensione di alimentazione o alimentatore spento.
1	Indicatore di stato della tensione di alimentazione di uscita	Indica lo stato della tensione di alimentazione per le uscite. OFF: alimentazione normale attiva. ON: errore di tensione di alimentazione o alimentatore spento.
2	Indicatore degli errori di comunicazione I/O standard	Indica la presenza o meno di errori nelle comunicazioni I/O standard. OFF: nessun errore. ON: è stato rilevato un errore in uno o più collegamenti standard.
3	Indicatore di stato comunicazione I/O standard	Indica se sono in corso o meno le comunicazioni I/O standard. L'indicatore è acceso se sono in corso comunicazioni regolari per tutti i collegamenti standard.
4	Indicatore degli errori di comunicazione I/O di sicurezza	Indica la presenza o meno di errori nelle comunicazioni I/O di sicurezza. OFF: nessun errore. ON: è stato rilevato un errore in uno o più collegamenti di sicurezza.
5	Indicatore di stato comunicazione I/O di sicurezza	Indica se sono in corso o meno le comunicazioni I/O di sicurezza. L'indicatore è acceso se sono in corso comunicazioni regolari per tutti i collegamenti di sicurezza.
6	Indicatore della modalità operativa	Indica la modalità operativa del controllore. OFF: il controllore non è in modalità Run. ON: il controllore è in modalità Run.
7	Indicatore dello stato del controllore	Indica lo stato del controllore. OFF: è presente un errore. ON: il controllore funziona regolarmente.

Stato degli ingressi locali

Quando il bit è attivo, lo stato dell'ingresso è normale. Quando il bit non è attivo, è stato rilevato un errore.

Stato del morsetto di ingresso di sicurezza locale

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Morsetto 7	Morsetto 6	Morsetto 5	Morsetto 4	Morsetto 3	Morsetto 2	Morsetto 1	Morsetto 0
1	Morsetto 15	Morsetto 14	Morsetto 13	Morsetto 12	Morsetto 11	Morsetto 10	Morsetto 9	Morsetto 8

Stato delle uscite locali

Quando il bit è attivo, lo stato dell'uscita è normale. Quando il bit non è attivo, è stato rilevato un errore.

Stato del morsetto di uscita di sicurezza locale

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Morsetto 7	Morsetto 6	Morsetto 5	Morsetto 4	Morsetto 3	Morsetto 2	Morsetto 1	Morsetto 0

Stato dell'uscita di test o della spia di muting

Quando il bit è attivo, lo stato dell'uscita di test è normale. Quando il bit non è attivo, è stato rilevato un errore.

Stato dell'uscita di test o della lampada di muting

Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Rilevato stato di disconnessione per il morsetto 3	Riservato			Morsetto 3	Morsetto 2	Morsetto 1	Morsetto 0

Stato di collegamento del controllore (funzione di slave di sicurezza)

Codice	Stato	Azione correttiva
00:0001	Comunicazione normale	Lo stato del collegamento I/O di sicurezza è normale.
01:0001	Timeout di collegamento I/O di sicurezza	Il collegamento I/O di sicurezza è in timeout. Verificare quanto segue. • È stata impostata la stessa velocità di trasmissione per tutti i nodi? • La lunghezza del cavo è corretta? • Il cavo è scollegato o allentato? • La resistenza di terminazione è stata installata solo su entrambe le estremità della linea principale? • Il livello di disturbo è eccessivo?
01:0106	Errore del proprietario del collegamento di uscita	Lo slave di sicurezza ha stabilito un collegamento I/O di sicurezza di uscita con un master di sicurezza che l'ultima volta aveva un indirizzo di nodo differente.
01:0109	Errore di dimensioni dei dati	Le dimensioni I/O dello slave di sicurezza impostate nel controllore SmartGuard non corrispondono alle dimensioni configurate nell'impostazione del collegamento di sicurezza del master di sicurezza. È possibile che l'impostazione I/O dello slave di sicurezza sia stata modificata, quindi eliminare e riconfigurare i collegamenti registrati nel master di sicurezza.
01:0110	Dispositivo non configurato	Lo slave di sicurezza non è stato configurato. Scaricare i parametri del dispositivo sullo slave di sicurezza.
01:0111	Errore di intervallo di pacchetto richiesto	L'intervallo di pacchetto richiesto impostato per il collegamento di sicurezza del master di sicurezza è inferiore alla durata del ciclo dello slave di sicurezza.
01:0113	Errore di numero di collegamenti	L'impostazione supera il numero massimo di collegamenti I/O di sicurezza supportati dallo slave di sicurezza. Verificare le impostazioni del collegamento di sicurezza del master di sicurezza interessato.
01:0114	Errore di ID fornitore o codice prodotto	I dati del dispositivo nel file di configurazione RSNetWorx per DeviceNet non corrispondono al dispositivo fisico nel sistema. Utilizzare la procedura guidata Safety Device Verification Wizard per verificare la corrispondenza tra il dispositivo nel sistema e il dispositivo nel file di configurazione. Se corrispondono, configurare di nuovo i collegamenti per il master di sicurezza.
01:0115	Errore di tipo di dispositivo	I dati del dispositivo nel file di configurazione RSNetWorx per DeviceNet non corrispondono al dispositivo fisico nel sistema. Utilizzare la procedura guidata Safety Device Verification Wizard per verificare la corrispondenza tra il dispositivo nel sistema e il dispositivo nel file di configurazione. Se corrispondono, configurare di nuovo i collegamenti per il master di sicurezza.
01:0116	Errore di versione firmware	I dati del dispositivo nel file di configurazione RSNetWorx per DeviceNet non corrispondono al dispositivo fisico nel sistema. Utilizzare la procedura guidata Safety Device Verification Wizard per verificare la corrispondenza tra il dispositivo nel sistema e il dispositivo nel file di configurazione. In caso di mancata corrispondenza, configurare di nuovo i collegamenti registrati per il master di sicurezza.

Codice	Stato	Azione correttiva
01:0117	Errore di percorso di collegamento	Sono stati impostati due o più collegamenti I/O di sicurezza single-cast o un collegamento I/O di sicurezza multi-cast con un intervallo di pacchetto richiesto differente per un I/O di slave di sicurezza. Per condividere un I/O di slave di sicurezza su uno slave di sicurezza con più master di sicurezza, uniformare l'intervallo di pacchetto richiesto e impostare il tipo di collegamento su multi-cast. Gli slave di sicurezza del controllore SmartGuard possono utilizzare un unico collegamento I/O di sicurezza single-cast per ogni I/O di slave di sicurezza. Impostare più percorsi di collegamento per l'I/O di slave di sicurezza del controllore. Se il problema persiste, eliminare e configurare di nuovo i collegamenti per il master di sicurezza.
01:031E	Errore di numero di collegamenti	L'impostazione del numero di collegamenti I/O di sicurezza supera il limite massimo supportato dallo slave di sicurezza. Modificare l'impostazione dei collegamenti di sicurezza per il master di sicurezza interessato. In particolare, verificare che non siano impostati più di 15 master di sicurezza per ogni collegamento multi-cast, per un totale massimo di 60.
01:031F	Errore di risorse di ID collegamento	È stato superato il numero massimo di ID collegamento (12) per un master di sicurezza. Fare clic su Advanced nella finestra di dialogo Safety Connection Properties. Selezionare la casella di controllo Request target device to allocate message IDs. Scaricare i parametri del dispositivo sul master di sicurezza.
01:07FF	Slave di sicurezza inesistente	È possibile che lo slave di sicurezza non sia stato aggiunto correttamente alla rete. Verificare che lo slave di sicurezza corrispondente sia online. In caso contrario, effettuare le seguenti verifiche: • L'indirizzo di nodo dello slave di sicurezza è corretto? • È stata impostata la stessa velocità di comunicazione per tutti i nodi? • La lunghezza del cavo è corretta? • Il cavo è scollegato o allentato? • La resistenza di terminazione è stata installata solo su entrambe le estremità della linea principale? • Il livello di disturbo è eccessivo?
01:080C	Autenticazione di sicurezza non corrispondente	L'autenticazione di sicurezza dello slave di sicurezza monitorato dal master di sicurezza non corrisponde all'autenticazione di sicurezza dello slave di sicurezza stesso. Ripristinare le impostazioni di default dello slave di sicurezza, quindi scaricare di nuovo i parametri del dispositivo. Se il problema persiste, eliminare e configurare di nuovo i collegamenti impostati nel master di sicurezza.
01:080E	Numero della rete di sicurezza (SNN) non corrispondente	Il numero SNN dello slave di sicurezza monitorato dal master di sicurezza non corrisponde al numero SNN dello slave di sicurezza stesso. Ripristinare le impostazioni di default dello slave di sicurezza, quindi scaricare i parametri corretti del dispositivo. Se il problema persiste, eliminare e configurare di nuovo i collegamenti impostati nel master di sicurezza.
D0:0001	Modalità di riposo	Il master di sicurezza del controllore SmartGuard è in modalità di riposo, pertanto non sono stati stabiliti i collegamenti I/O di sicurezza. Impostare la modalità operativa del controllore SmartGuard su Execute.

Categorie di errore

Gli errori del controllore possono essere classificati in errori reversibili, errori di interruzione e errori gravi.

Categorie di errore del controllore

Categoria di errore	Descrizione
Errore reversibile	Un errore che blocca tutti i morsetti di collegamento di I/O locale o di sicurezza, attivandone lo stato di sicurezza. Il controllore continua a funzionare in modalità Run.
Errore di interruzione	Il controllore esce dalla modalità Run per entrare in modalità di riposo e viene attivato lo stato di sicurezza per tutti gli I/O di sicurezza. Sono supportate le comunicazioni tramite messaggi espliciti e funzioni limitate del software RSNetWorx for DeviceNet per consentire all'utente di verificare lo stato di errore.
Errore grave	Quando si verifica questo tipo di errore viene completamente interrotto il funzionamento del controllore. Vedere pagina 190 per gli errori di download. Vedere Errori di ripristino e azioni correttive per gli errori di ripristino. Vedere Errori di modifica della modalità e azioni correttive per gli errori che possono verificarsi durante la modifica delle modalità.

Tabella cronologica degli errori

Al rilevamento di un errore, viene creato un record nella tabella cronologica degli errori nella RAM del controllore. Se il numero dei record di errore supera la cifra massima di 100, i record più obsoleti vengono eliminati consecutivamente e i dati di errore più recenti vengono memorizzati come nuovi record.

Nella tabella cronologica degli errori viene memorizzato lo stato del controllore al momento dell'errore oltre all'ora (tempo totale di funzionamento del controllore[(1)]) e all'indirizzo di nodo in cui si è verificato l'errore.

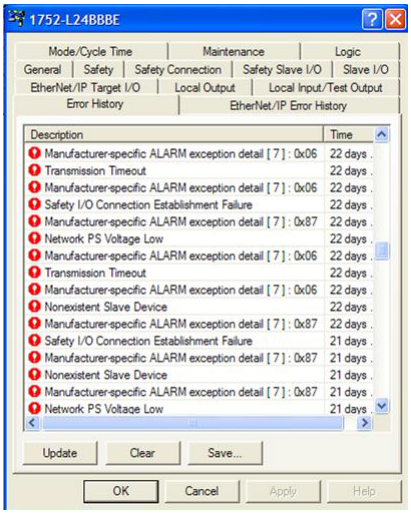
Area di memoria della cronologia errori

La descrizione di un errore viene registrata come voce della cronologia errori nella RAM del controllore. Se l'errore è grave, viene salvato anche nella memoria non volatile. La cronologia errori registrata nella memoria non volatile viene conservata anche quando il controllore non è alimentato o viene riavviato.
La cronologia errori nella memoria non volatile viene copiata nella RAM del controllore quando il controllore viene spento e riacceso. La cronologia errori nella RAM viene letta durante la lettura della cronologia errori dal software RSNetWorx per DeviceNet. Tuttavia, quando viene cancellata la cronologia errori, le cronologie errori nella RAM e nella memoria non volatile vengono cancellate.

Visualizzazione della tabella cronologica degli errori per il controllore 1752-L24BBB

Attenersi alla seguente procedura per visualizzare la cronologia errori in tempo reale utilizzando il software RSNetWorx for DeviceNet con il controllore online.

1. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Properties.
2. Fare clic sulla scheda Error History.



(1) Il tempo totale di funzionamento del controllore viene registrato come tempo complessivo in incrementi di 6 minuti per cui l'alimentatore V0, G0 è attivo. Il tempo totale di funzionamento viene cancellato dal comando di ripristino del controllore.

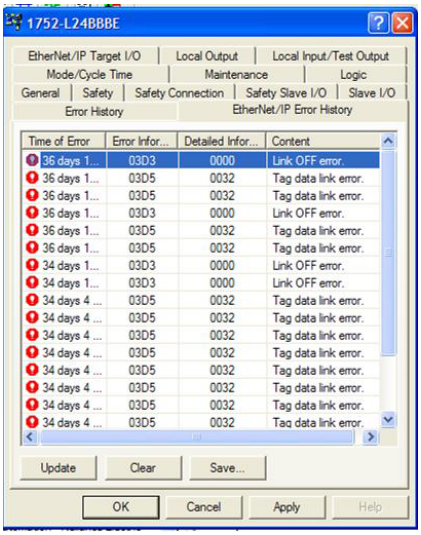
a. Fare clic su Save per salvare i dati della cronologia errori. I dati possono essere salvati anche in un file CSV separato.
b. Fare clic su Clear per cancellare la cronologia errori salvata nel controllore.
c. Fare clic su Update per aggiornare le informazioni sulla cronologia errori.

Visualizzazione della tabella cronologica degli errori EtherNet/IP per il controllore 1752-L24BBBE

Attenersi alla seguente procedura per visualizzare la cronologia errori in tempo reale utilizzando il software RSNetWorx for DeviceNet con il controllore online.

1. Fare clic con il pulsante destro del mouse sul controllore SmartGuard e selezionare Properties.

2. Fare clic sulla scheda EtherNet/IP Error History.



a. Fare clic su Save per salvare i dati della cronologia errori. I dati possono essere salvati anche in un file CSV separato.
b. Fare clic su Clear per cancellare la cronologia errori salvata nel controllore.
c. Fare clic su Update per aggiornare le informazioni sulla cronologia errori.

Tabella cronologica degli errori EtherNet

Codice d'errore	Errore	Codice in dettaglio		Display a 7 segmenti
		1° byte[1]	2° byte[1]	
0602	Memoria unità bus CPU	01: Errore di lettura	Variabile	E9<->n4
		02; Errore di scrittura		
020F	Comunicazione controllore	00	01	F4<->n4
0211	Indirizzo IP duplicato	02	Byte basso indirizzo IP	F0<->n4
021A	Errore logico tabella di impostazione	00	Variabile	UF
03C4	Connessione server	04; BOOTP	01; Host specifico inesistente	E3<0>n4
			07: Errore di trasmissione	
			08: Errore di ricezione	
			0A: Errore indirizzo IP	
03D0	Impostazione di base Ethernet	01: Errore di impostazione Ethernet	01: Errore di checksum	F2<->n4
			11: Impostazione incoerente	
			12; Velocità di trasmissione specifica non supportata	
		02: Errore di impostazione di base TCP/IP	01: Errore di checksum	
			11: Indirizzo IP non valido	
			12: Maschera di sottorete non valida	
			13: Indirizzo gateway di default non valido	
			14: Server dei nomi primario non valido	
			15: Server dei nomi secondario non valido	
			16: Server dominio non valido	
			17: Nome host non valido	
03D5	Collegamento dati tag	00	Byte basso indirizzo IP	L9<->n4
03D3	Collegamento OFF	00	00	E1<->n4

(1) Nella colonna "Detailed Information" della scheda EtherNet/IP Error History, la combinazione tra il primo e il secondo byte compare come un singolo carattere 4 esad. Per gli esempi, vedere la finestra di dialogo nella sezione Visualizzazione della tabella cronologica degli errori EtherNet/IP per il controllore 1752-L24BBBE.

Messaggi della cronologia errori e azioni correttive

Utilizzare i messaggi della cronologia errori per identificare e correggere gli errori.

Messaggi di errori relativi ai guasti del sistema del controllore

Messaggio	Descrizione	Azione correttiva
Guasto del sistema	Si è verificato un guasto del sistema.	Sostituire il controllore se viene segnalato di nuovo un guasto del sistema dopo aver spento e riacceso il sistema.
Invalid Configuration	La configurazione non è valida.	La configurazione corrente è diversa dalla configurazione originaria. Verificare e riconfigurare.

Messaggi di errore relativi alla programmazione

Messaggio	Descrizione	Azione correttiva
Function Block Status Error	È stato impostato un ingresso di segnale incompatibile come condizione di ingresso nei parametri del blocco funzione.	Verificare gli ingressi specificati nel blocco funzione o nella logica di programma.

Messaggi di errore relativi alla comunicazione DeviceNet

Messaggio	Descrizione	Azione correttiva
Switch Setting Mismatch	Le impostazioni dei selettori non corrispondono.	Verificare che l'indirizzo di nodo sia lo stesso dell'ultima configurazione. In caso contrario, reimpostare l'indirizzo di nodo originario o riconfigurarlo. Se l'errore persiste, sostituire il controllore.
Duplicate MAC ID	Uno o più indirizzi di nodo sono duplicati.	Verificare l'indirizzo di nodo degli altri nodi. Correggere la configurazione in modo che ogni indirizzo di nodo venga utilizzato una sola volta, quindi spegnere e riaccendere l'alimentatore.
Network PS Voltage Low	La tensione di alimentazione di rete è bassa.	Verificare che la tensione di alimentazione impostata rientri nell'intervallo consentito. Verificare che tutti i cavi siano collegati.
Bus Off	Le comunicazioni sono state interrotte a causa di errori di dati frequenti.	Verificare che la velocità di comunicazione sia identica per tutti i nodi. Verificare che i cavi della linea principale o delle linee di diramazione non siano troppo lunghi. Verificare che tutti i cavi siano collegati e non allentati. Verificare che la resistenza di terminazione sia stata installata solo su entrambe le estremità della linea principale. Verificare che il livello di disturbi nel sistema non sia eccessivo.
Transmission Timeout	Timeout della trasmissione.	
Standard I/O Connection Timeout	Timeout del collegamento I/O standard.	
Relevant Safety I/O Communication Stopped Because of a Safety I/O Communication Error	Il collegamento I/O di sicurezza corrispondente è stato interrotto in seguito al timeout di un collegamento I/O di sicurezza.	
All Safety I/O Communication Stopped Because of a Safety I/O Communication Error	Tutti i collegamenti I/O di sicurezza sono stati interrotti in seguito al timeout di un collegamento I/O di sicurezza.	
Safety I/O Connection Timeout	Il collegamento I/O di sicurezza è in timeout.	
Nonexistent Slave Device	Nessun dispositivo slave nel sistema.	
Safety I/O Connection Establishment Failure	Si è verificato un errore durante il tentativo di stabilire un collegamento di sicurezza.	Verificare che il dispositivo sia configurato e funzioni correttamente.
Invalid Slave Device	Un dispositivo slave non autorizzato è in rete (errore di verifica).	Verificare il dispositivo slave e collegare un dispositivo slave adatto.
EM Transmission Error (Duplicate MAC ID)	Non è possibile effettuare la trasmissione a causa di un indirizzo di nodo duplicato.	Verificare l'indirizzo di nodo degli altri nodi. Correggere la configurazione in modo che ogni indirizzo di nodo venga utilizzato una sola volta, quindi spegnere e riaccendere l'alimentatore.
EM Transmission Error (Invalid Header)	Non è possibile effettuare la trasmissione a causa di un'intestazione non valida.	Verificare l'indirizzo di nodo, l'ID classe e l'ID istanza del messaggio di trasmissione.

Messaggi di errore relativi alla comunicazione DeviceNet

Messaggio	Descrizione	Azione correttiva
EM Transmission Error (Device Offline)	Non è possibile effettuare la trasmissione poiché il dispositivo locale non è in rete.	Verificare che la velocità di comunicazione sia identica per tutti i nodi. Verificare che i cavi della linea principale o delle linee di diramazione non siano troppo lunghi. Verificare che la resistenza di terminazione sia stata installata solo su entrambe le estremità della linea principale. Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi. Verificare che la tensione di alimentazione per la sorgente di alimentazione della rete sia impostata su un valore compreso nell'intervallo consentito.
EM Transmission Error (Message ID Error)	Non è possibile effettuare la trasmissione a causa di un errore di ID messaggio.	
EM Transmission Error (Response Timeout)	Non è possibile effettuare la trasmissione a causa del timeout di risposta.	
EM Transmission Error (Destination Device Absence)	Non è possibile effettuare la trasmissione poiché il dispositivo di destinazione non è in rete.	Verificare l'indirizzo di nodo del nodo di destinazione e l'indirizzo di nodo del messaggio di trasmissione. Verificare che la tensione di alimentazione per il nodo di destinazione sia impostata su un valore compreso nell'intervallo consentito. Verificare che la velocità di comunicazione sia identica per tutti i nodi. Verificare che i cavi della linea principale e delle linee di diramazione non siano troppo lunghi. Verificare che tutti i cavi siano collegati e non allentati. Verificare che la resistenza di terminazione sia stata installata solo su entrambe le estremità della linea principale. Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi.
EM Transmission Error (Destination Buffer Full)	Non è possibile effettuare la trasmissione poiché il buffer di destinazione è occupato.	Verificare le dimensioni di ricezione del messaggio nel nodo di destinazione.
EM Transmission Error (Command Length Error)	Non è possibile effettuare la trasmissione poiché il comando supera la lunghezza massima consentita.	Verificare le dimensioni del messaggio di risposta dalla destinazione. Verificare anche che le dimensioni previste per la risposta nel messaggio di richiesta siano corrette.
EM Transmission Error (New Request Received)	Il messaggio è stato eliminato poiché è stata ricevuta una nuova richiesta.	Nessuna.
Received Error Response (UEM)	Viene ricevuta una risposta di errore quando viene utilizzata la funzione di messaggi espliciti dell'utente.	Verificare che il servizio specificato o le dimensioni dei dati nel messaggio esplicito dell'utente corrispondano alle specifiche dell'oggetto di destinazione.

Messaggi di errori relativi ai guasti del sistema del controllore EtherNet/IP

Messaggio	Descrizione	Azione correttiva
System Failure	Si è verificato un guasto del sistema.	Spegnere e riaccendere l'alimentatore. Se il guasto persiste, sostituire il controllore.
	Errore di memoria EtherNet/IP.	
	Errore del controllore di comunicazione EtherNet/IP.	
	Stesso indirizzo IP impostato per un altro dispositivo in rete.	Controllare gli indirizzi IP degli altri dispositivi ed impostare un indirizzo diverso da tutti gli altri.
	Errore logico nella tabella di impostazione.	Controllare la configurazione. Se il guasto persiste, sostituire il controllore.
	Errore di connessione server BOOTP.	Verificare che il cavo sia collegato correttamente. Verificare che il server BOOTP funzioni normalmente.
	Errore logico impostazione di base EtherNet/IP.	Controllare la configurazione. Se il guasto persiste, sostituire il controllore.
	Errore di comunicazione target standard EtherNet/IP.	Verificare che le impostazioni di comunicazione siano le stesse per tutti i nodi. Verificare che i cavi non siano scollegati o piegati. Verificare che l'origine sia alimentata.
	Errore Collegamento Off.	Verificare che le impostazioni di comunicazione siano le stesse per tutti i nodi. Verificare che i cavi non siano scollegati o piegati. Verificare che l'hub sia alimentato.

Messaggi di errore relativi all'alimentazione I/O

Messaggio	Descrizione	Azione correttiva
Input PS Voltage Low	L'alimentatore I/O (V1, G1) non è collegato.	Verificare che la tensione di alimentazione impostata rientri nell'intervallo consentito. Verificare che tutti i cavi siano collegati.
Output PS Voltage Low	L'alimentatore I/O (V2, G2) non è collegato.	

Messaggi di errore relativi agli ingressi di sicurezza

Messaggio	Descrizione	Azione correttiva
External Test Signal Failure at Safety Input	Si è verificato un guasto del cablaggio esterno nell'ingresso di sicurezza.	Verificare che il cavo del segnale di ingresso non sia a contatto con l'alimentazione (polo positivo).
Discrepancy Error at Safety Input	È stata rilevata una discrepanza tra due ingressi configurati come Canale duale.	Verificare che il cavo del segnale di ingresso non presenti un guasto verso terra. Verificare che il cavo del segnale di ingresso non sia scollegato. Verificare l'assenza di cortocircuito tra i cavi di segnale di ingresso. Verificare che non si sia verificato un guasto nel dispositivo collegato. Verificare che il valore impostato per il tempo di discrepanza sia valido. Per il ripristino da questo stato di errore, è necessario che il tempo di mantenimento dello stato di errore dell'ingresso sia trascorso e che la causa dell'errore sia stata eliminata. Gli ingressi di sicurezza di destinazione devono essere disattivati. Per modificare il tempo di discrepanza, è necessario riconfigurare l'ingresso di sicurezza.
Internal Input Failure at Safety Input	Si è verificato un errore del circuito interno per l'ingresso di sicurezza.	Sostituire l'unità se viene segnalato di nuovo un guasto del sistema dopo aver spento e riacceso l'alimentatore.

Messaggi di errore relativi all'uscita di test

Messaggio	Descrizione	Azione correttiva
Overload Detected at Test Output	Viene assorbita troppa corrente in corrispondenza dell'uscita di test.	Verificare se il cavo del segnale di uscita presenta un guasto verso terra o se è sovraccarico.
Stuck-at-high Detected at Test Output	L'uscita di test è bloccata nello stato on.	Verificare se la sorgente di alimentazione fa contatto con il cavo del segnale di uscita. Una volta trascorso il tempo di mantenimento dello stato di errore, disattivare l'ingresso dopo aver corretto l'errore. L'errore viene ripristinato. Se i cavi non presentano alcun problema, sostituire l'unità.
Under-current Detected Using Muting Lamp	È stato rilevato un errore di superamento del limite inferiore della corrente per l'uscita di test T3.	Verificare se il cavo del segnale di uscita è disconnesso o se la spia di muting è danneggiata. Se i cavi non presentano alcun problema, verificare gli indicatori di stato.

Messaggi di errore relativi all'uscita di sicurezza

Messaggio	Descrizione	Azione correttiva
Over Current Detected at Safety Output	È stata rilevata una sovracorrente nell'uscita di sicurezza.	Verificare l'assenza di sovracorrente per l'uscita.
Short Circuit Detected at Safety Output	È stato rilevato un cortocircuito nell'uscita di sicurezza.	Verificare che il cavo del segnale di uscita non presenti un guasto verso terra.
Stuck-at-high Detected at Safety Output	L'uscita di sicurezza è bloccata nello stato alto.	
Cross Connection Detected at Safety Output	È stato rilevato un cortocircuito tra i cavi di segnale di uscita in un'uscita di sicurezza.	Verificare che il cavo del segnale di uscita non sia a contatto con l'alimentazione (polo positivo). Verificare l'assenza di cortocircuito tra i cavi di segnale di uscita.
Dual Channel Violation at Safety Output	Si è verificato un errore di dati di uscita in un'uscita di sicurezza.	Verificare che i dati delle due uscite nella modalità Canale duale siano stati configurati come canali equivalenti.

Errori di download e azioni correttive

Il controllore può restituire una risposta di errore durante il download dei dati di configurazione sul controllore. Utilizzare i messaggi visualizzati nel software RSNetWorx per DeviceNet per identificare l'errore.

Messaggi di errore relativi al download del software RSNetWorx per DeviceNet e azioni correttive

Messaggio	Descrizione	Azione correttiva
Cannot be executed in the current mode.	Si è verificato un errore irreversibile (interruzione) e l'indicatore MS (stato del modulo) lampeggia in rosso.	Verificare che i selettori siano impostati correttamente. Altrimenti, eseguire il ripristino per cancellare i dati di configurazione.
The device is locked.	La configurazione è bloccata e l'indicatore di stato LOCK (blocco) è acceso.	Sbloccare il dispositivo.
The TUNID is different.	Il numero della rete di sicurezza (SNN) non è stato impostato dopo il ripristino del dispositivo (l'indicatore dello stato della rete NS lampeggia in verde e rosso) oppure il numero SNN nel dispositivo non corrisponde al numero SNN scaricato dal software RSNetWorx for DeviceNet.	1. Ripristinare le impostazioni di default del dispositivo e scaricare di nuovo i parametri. Il numero SNN potrebbe essere diverso rispetto a quello degli altri dispositivi. Se sul display alfanumerico del controllore viene visualizzata l'indicazione d6 e viene visualizzato il messaggio Safety I/O Connection Establishment Failure nella tabella cronologica degli errori dopo la modifica della modalità operativa, passare al punto successivo. 2. Selezionare Network > Upload from Network nel software RSNetWorx per DeviceNet. Uniformare il numero SNN su tutta la rete e ripristinare le impostazioni di default di tutti i dispositivi. Dopo il completamento del ripristino, scaricare di nuovo i parametri sui dispositivi.
Privilege violation.	1. La password utilizzata non dispone dei privilegi per la modifica della configurazione. 2. Si è tentato di impostare la modalità stand alone tramite un collegamento DeviceNet.	1. Verificare che la password sia corretta. 2. Collegarsi al controllore SmartGuard tramite un connettore USB e scaricare di nuovo la configurazione. Con il controllore 1752-L24BBBE, è possibile scaricare anche mediante la rete EtherNet/IP.
Cannot be executed in the current device mode.	I dati vengono scaricati da più istanze del software RSNetWorx per DeviceNet.	Attendere il completamento del download dall'altra istanza.
An error was found during parameter check.	È stata rilevata un'incongruenza tra i parametri di configurazione.	Correggere le impostazioni dei parametri. Verificare quanto segue. • Un parametro temporale configurato per un blocco funzione è inferiore alla durata del ciclo del controllore. • L'intervallo di pacchetto richiesto (RPI) per un collegamento di sicurezza è inferiore alla durata del ciclo. • Un ingresso di sicurezza è configurato come 'Used with test pulse', ma la sorgente di test non è impostata. • Quando gli ingressi di sicurezza sono stati configurati per la modalità Canale duale, un ingresso è stato configurato come ingresso standard, ma l'altro presenta un'impostazione diversa. • Quando gli ingressi di sicurezza sono stati configurati per la modalità Canale duale, un ingresso è stato configurato per non essere utilizzato, ma l'altro presenta un'impostazione diversa. • Quando le uscite di sicurezza sono state configurate per la modalità Canale duale, un'uscita è stata configurata per non essere utilizzata, ma l'altra presenta un'impostazione diversa. • In una configurazione degli I/O di sicurezza, è stato impostato un parametro che ha causato il superamento del numero massimo di ID collegamento (12) del master. Fare clic su Advanced nella finestra di dialogo Safety Connection Properties. Selezionare la casella di controllo Request target device to allocate message IDs.

Messaggi di errore relativi al download del software RSNetWorx per DeviceNet e azioni correttive

Messaggio	Descrizione	Azione correttiva
The data used by the logic program is not aligned with other data.	In seguito alla modifica della configurazione di rete, i dati utilizzati dalla logica di programma non corrispondono agli altri dati.	Utilizzare Logic Editor per verificare le posizioni I/O modificate e ripristinare i dati.
Could not access the device.	Il controllore è stato ripristinato da un altro nodo durante l'esecuzione del download e il numero della rete di sicurezza (SNN) non è stato ancora impostato. L'indicatore di stato NS (stato della rete) lampeggia in rosso/verde.	Impostare il numero SNN e scaricare di nuovo i dati.
Could not open connection.	Impossibile creare un collegamento al controllore durante un download sul controllore tramite la rete DeviceNet o EtherNet/IP.	1. Verificare che l'alimentatore del dispositivo sia acceso e riprovare a scaricare i dati. 2. Impostare la modalità operativa del master di sicurezza su Riposo. 3. È anche possibile che disturbi o altri fattori abbiano reso le comunicazioni instabili. • Verificare che la velocità di comunicazione sia identica per tutti i nodi. • Verificare che i cavi della linea principale e delle linee di diramazione non siano troppo lunghi. • Verificare che tutti i cavi siano collegati e non allentati. • Verificare che i resistori di terminazione siano installati su entrambe le estremità della linea principale. • Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi.
Message could not be sent.	Impossibile creare un collegamento al controllore durante un download sul controllore tramite la porta USB o la rete EtherNet/IP.	Verificare che l'alimentatore del dispositivo sia acceso e riprovare a scaricare i dati.
Connection failed.	Tentata configurazione di un dispositivo sulla rete DeviceNet o EtherNet/IP tramite la porta USB ma risulta impossibile stabilire la connessione.	Verificare che l'alimentatore del dispositivo sia acceso e riprovare a scaricare i dati. È anche possibile che disturbi o altri fattori abbiano reso le comunicazioni instabili. • Verificare che la velocità di comunicazione sia identica per tutti i nodi. • Verificare che i cavi della linea principale e delle linee di diramazione non siano troppo lunghi. • Verificare che tutti i cavi siano collegati e non allentati. • Verificare che i resistori di terminazione siano installati su entrambe le estremità della linea principale. • Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi.
Program incomplete. Start Logic Editor and check program.	In un blocco funzione utilizzato nella logica di programma sono presenti uscite o ingressi aperti.	In Logic Editor del software RSNetWorx per DeviceNet, collegare le uscite o gli ingressi aperti oppure modificare il numero di I/O impostati per il blocco funzione in modo da eliminare le uscite o gli ingressi non collegati.

Errori di ripristino e azioni correttive

Il controllore può restituire una risposta di errore durante il ripristino. Utilizzare i messaggi visualizzati nel software RSNetWorx per DeviceNet per identificare l'errore.

Messaggi di errore relativi al ripristino del software RSNetWorx per DeviceNet e azioni correttive

Messaggio	Descrizione	Azione correttiva
Cannot execute in current mode.	Non è possibile eseguire il ripristino specificato se il controllore è nello stato corrente.	Modificare la modalità operativa oppure lo stato di blocco della configurazione, quindi eseguire il ripristino.
The device has a different TUNID. the device TUNID will be used to reset. Is that OK?	Il numero della rete di sicurezza (SNN) salvato nel dispositivo non corrisponde al numero SNN specificato dal software RSNetWorx per DeviceNet.	Verificare la corrispondenza dell'ID MAC del dispositivo. In caso positivo, ripristinare il numero SNN salvato nel dispositivo.
Access error.	La password utilizzata non fornisce i privilegi per la modifica delle configurazioni.	Accertarsi che venga utilizzata la password corretta.
The device cannot be accessed or the device type or password is different.	1. Il dispositivo è stato appena ripristinato o spento e riacceso e non è ancora pronto per la comunicazione. 2. Il dispositivo specificato per il ripristino non supporta questo servizio. 3. I dati di configurazione sono bloccati. L'indicatore di stato LOCK (blocco) è acceso. 4. Il dispositivo esegue comunicazioni I/O di sicurezza e non può eseguire la richiesta specificata.	1. Verificare che il dispositivo sia pronto per la comunicazione ed effettuare un nuovo tentativo di ripristino. 2. Verificare che l'ID MAC del dispositivo sia corretto. 3. Rimuovere il blocco, quindi eseguire il ripristino specificato. 4. Impostare la modalità operativa del relativo master di sicurezza su Riposo, quindi eseguire il ripristino specificato.
Connection failed.	Tentato ripristino di un dispositivo sulla rete DeviceNet o EtherNet/IP tramite la porta USB ma è impossibile stabilire la connessione.	Verificare che l'alimentatore del dispositivo sia acceso ed effettuare un nuovo tentativo di ripristino. È anche possibile che disturbi o altri fattori abbiano reso le comunicazioni instabili. • Verificare che la velocità di comunicazione sia identica per tutti i nodi. • Verificare che i cavi della linea principale e delle linee di diramazione non siano troppo lunghi. • Verificare che tutti i cavi siano collegati e non allentati. • Verificare che i resistori di terminazione siano installati su entrambe le estremità della linea principale. • Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi.

Errori di modifica della modalità e azioni correttive

Il controllore può restituire una risposta di errore quando le modalità vengono modificate. Utilizzare i messaggi visualizzati nel software RSNetWorx per DeviceNet per identificare l'errore.

Messaggi di errore relativi alla modifica delle modalità del software RSNetWorx per DeviceNet e azioni correttive

Messaggio	Descrizione	Azione correttiva
Cannot be executed in the current mode.	1. Il dispositivo non è stato configurato. 2. Si è verificato un errore irreversibile (interruzione).	1. Scaricare i parametri del dispositivo. 2. Impostare correttamente i selettori del dispositivo oppure eseguire il ripristino per cancellare i dati di configurazione, quindi scaricare di nuovo i parametri del dispositivo.
Already set to the specified mode.	Il dispositivo è già nella modalità specificata.	
The device has a different TUNID.	Il numero della rete di sicurezza (SNN) salvato nel dispositivo non corrisponde al numero SNN specificato dal software RSNetWorx per DeviceNet.	Verificare la corrispondenza dell'ID MAC. In caso positivo, l'indirizzo di rete del dispositivo non corrisponde all'indirizzo di rete specificato nel file di configurazione di RSNetWorx per DeviceNet. Caricare la rete nel software RSNetWorx per DeviceNet in modo che l'indirizzo di rete corrisponda.
Access error.	La password utilizzata non fornisce i privilegi per la modifica della modalità operativa.	Accertarsi che venga utilizzata la password corretta.
The device cannot be accessed, or the device type or password is different.	1. Il dispositivo è stato appena ripristinato o spento e riacceso e non è ancora pronto per la comunicazione. 2. È possibile che il dispositivo per cui è stata richiesta la modifica di modalità non supporti questo servizio.	1. Verificare che il dispositivo sia pronto per la comunicazione e ritentare la modifica della modalità. 2. Verificare che l'ID MAC del dispositivo sia corretto.
Connection failed.	Tentata modifica della modalità operativa di un dispositivo sulla rete DeviceNet o EtherNet/IP tramite la porta USB, ma risulta impossibile stabilire la connessione.	Verificare che l'alimentatore del dispositivo sia acceso e ritentare la modifica della modalità. È anche possibile che disturbi o altri fattori abbiano reso le comunicazioni instabili. • Verificare che la velocità di comunicazione sia identica per tutti i nodi. • Verificare che i cavi della linea principale e delle linee di diramazione non siano troppo lunghi. • Verificare che tutti i cavi siano collegati e non allentati. • Verificare che i resistori di terminazione siano installati su entrambe le estremità della linea principale. • Prendere le precauzioni appropriate per evitare un livello eccessivo di disturbi.

Note:

Specifiche dei controllori

Introduzione

Questa appendice contiene le specifiche per i controllori SmartGuard 600.

Argomento	Pagina
Caratteristiche tecniche generali	195
Specifiche ambientali	197
Certificazioni	199

Caratteristiche tecniche generali

Attributo	1752-L24BBB	1752-L24BBBE
Dimensioni (AxLaxP), circa	99,0[4] x 99,4 x 131,4 mm[5]	99,0[4] x 113,0 x 131,4 mm[5]
Peso, circa	460 g	575 g
Carico di corrente DeviceNet, max	15 mA a 24 V CC	
Tensione di alimentazione[1]	20,4…26,4 V CC (24 V CC, -15…10%)	
Corrente di spunto – alimentatore unità	4,8 A di picco per 600 µs a V0/G0	
Corrente di spunto – alimentatore ingressi di sicurezza	2,6 A di picco per 3 ms a V1/G1	
Campo di tensione DeviceNet	11…25 V CC	
Consumo di corrente (V0 – circuito logico interno)	230 mA a 24 V CC	280 mA a 24 V CC
Protezione da sovraccarico	Spegnimento delle uscite interessate con riconnessione ciclica	
Tensione di isolamento	50 V, Prove di tipo isolamento funzionale a 600 V CA per 60 s, tra tutti i gruppi	
Tipo di cavo	Rame	
Categoria di cablaggio[2]	2 – sulle porte di alimentazione, segnale e comunicazione	2 – su alimentazione, 1 – su segnale, 1 – porta di comunicazione
Sezione del cavo	Per l'alimentatore e gli I/O, utilizzare un cavo a filo unico da 0,2-2,5 mm^2 mm (12-24 AWG) o un cavo flessibile standard da 0,34-1,5 mm^2 (16-22 AWG). Prima di effettuare il collegamento, preparare i cavi standard fissando le boccole con ghiere isolanti in plastica (conformi allo standard DIN 46228-4) Per collegamenti EtherNet: Connettore RJ45 conformemente alla norma IEC 60603-7, 2 o 4 coppie, cavo di Categoria 5e minimo conformemente a TIA 569-B.1 o cavo di Categoria 5 conformemente a ISO/IEC 24701	
Coppia di serraggio dei morsetti I/O	0,56-0,79 N•m	
Codice temperatura nordamericano	T4A	
Tipo di ingresso	Assorbimento di corrente	
Tensione, ingresso stato on, min	11 V CC	

Attributo	1752-L24BBB	1752-L24BBBE
Tensione, ingresso stato off, max	5 V CC	
Corrente, ingresso stato off, max	1 mA	
Corrente di ingresso	4,5 mA	
Impedenza di ingresso	2,6 kΩ	
Tipo uscita di test	Erogazione di corrente	
Corrente di uscita pulse test(3)	0,7 A	
Corrente di picco uscita di prova	0,7 A	
Tensione stato off pulse test, max	1,2 V	
Corrente di dispersione uscita pulse test, max	0,1 mA	
Corrente di uscita lampada di muting (T3) • Più di 25 mA • Meno di 5 mA	 • Funzionamento normale (per evitare guasti quando utilizzato come uscita di una lampada di muting) • Guasto (indicazione di guasto generata quando utilizzato come uscita di una lampada di muting)	
Tipo di uscita	Erogazione di corrente	
Corrente di uscita	0,5 A	
Corrente di uscita di picco	0,5 A	
Tensione, uscita stato off, max	1,2 V	
Corrente di dispersione, uscita stato off, max	0,1 mA	
Dissipazione termica	9,3 W a carico max	

Attributo	1752-L24BBB	1752-L24BBBE
Comunicazione Ethernet		
Connessioni CIP	Non applicabile	2
Autonegoziazione	Non applicabile	Supportata
Frequenza dati	Non applicabile	10/100 Mbps
Duplex	Non applicabile	Full/half
Larghezza di banda ammissibile comunicazione unità	Non applicabile	3000 pps(6)
Comunicazione messaggi espliciti	Non applicabile	502 byte(7)

(1) V0/G0 per circuito logico interno; V1/G1 per dispositivi di ingresso esterni ed uscite di prova; V2/G2 per dispositivi di uscita esterni.

(2) Utilizzare le informazioni fornite sulla categoria del conduttore per pianificare l'instradamento dei conduttori. Consultare Criteri per il cablaggio e la messa a terra in automazione industriale, pubblicazione 1770-4.1.

(3) Corrente totale T0...T3 contemporaneamente: 1,4 A.

(4) L'altezza include i connettori del terminale.

(5) La profondità include il connettore DeviceNet.

(6) PPS è l'acronimo di Packets Per Second (pacchetti al secondo). Indica il numero di pacchetti inviati o ricevuti che possono essere elaborati ogni secondo.

(7) La lunghezza massima del messaggio per connessione classe 3 e connessione UCMM.

Specifiche ambientali

Attributo	1752-L24BBB	1752-L24BBBE
Temperatura, stoccaggio	IEC 60068-2-1 (Test Ab, senza imballo, a riposo, freddo), IEC 60068-2-2 (Test Bb, senza imballo, a riposo, caldo secco), IEC 60068-2-14 (Test Na, senza imballo, a riposo, shock termico): -40…70 °C	
Temperatura, funzionamento	IEC 60068-2-1 (Test Ad, funzionamento con freddo), IEC 60068-2-2 (Test Bd, funzionamento con caldo secco), IEC 60068-2-14 (Test Nb, funzionamento con shock termico): -10…55 °C	
Umidità relativa	IEC 60068-2-30 (Test Db, senza imballo, a riposo, caldo umido): 10…95% senza condensa	
Vibrazioni	IEC 60068-2-6 (Test Fc, in funzione): 0,35 mm a 10…57 Hz 5 g a 57…150 Hz	IEC 60068-2-6 (Test Fc, in funzione): 5 g a 10…500 Hz
Urti, in funzione	IEC 60068-2-27 (Test Ea, urto senza imballo): 15 g	
Urti, a riposo	IEC 60068-2-27 (Test Ea, urto senza imballo): 30 g	
Grado di protezione custodia	IP20	
Emissioni	CISPR 11: Gruppo 1, Classe A	
Immunità ESD	IEC 61000-4-2: • scariche da 4 kV a contatto • scariche da 8 kV in aria	IEC 61000-4-2: • scariche da 6 kV a contatto • scariche da 8 kV in aria

Attributo	1752-L24BBB	1752-L24BBBE
Immunità RF irradiate	IEC 61000-4-3: • 10 V/m con onda sinusoidale di 1 kHz, 80% AM da 80 a 1000 MHz • 10 V/m con onda sinusoidale di 1 kHz, 80% AM da 1,4 a 2,0 GHz • 10 V/m con 50% impulso a 200 Hz, 100% AM a 900 MHz • 10 V/m con 50% impulso a 200 Hz, 100% AM a 1200 MHz • 3 V/m con onda sinusoidale di 1 kHz, 80% AM da 2000 a 2700 MHz	IEC 61000-4-3: • 10 V/m con onda sinusoidale di 1 kHz, 80% AM da 80 a 1000 MHz • 10 V/m con onda sinusoidale di 1 kHz, 80% AM da 1,4 a 2,0 GHz • 20 V/m con 50% impulso a 200 Hz, 100% AM a 800, 900, 1200 MHz • 3 V/m con onda sinusoidale di 1 kHz, 80% AM da 2000 a 2700 MHz
Immunità EFT/B	IEC 61000-4-4: • ±2 kV a 5 kHz sulle porte di potenza • ±2 kV a 5 kHz sulle porte di segnale • ±2 kV a 5 kHz sulle porte di comunicazione	IEC 61000-4-4: • ±2 kV a 5 kHz sulle porte di potenza • ±1 kV a 5 kHz sulle porte di segnale • ±1 kV a 5 kHz sulle porte di comunicazione
Immunità ai transitori di picco	IEC 61000-4-5: • ±1 kV fase-fase (DM) e ±2 kV fase-terra (CM) sulle porte di potenza • ±1 kV fase-fase (DM) e ±2 kV fase-terra (CM) sulle porte di segnale • ±1 kV fase-terra (CM) sulle porte di comunicazione	IEC 61000-4-5: • ±500 V fase-fase (DM) e ±1 kV fase-terra (CM) sulle porte di potenza • ±1 kV fase-terra (CM) sulle porte di segnale • ±1 kV fase-terra (CM) sulle porte di comunicazione
Immunità RF condotte	IEC 61000-4-6: • 10 V efficace con onda sinusoidale di 1 kHz, 80% AM da 150 kHz a 80 MHz	

Certificazioni

Certificazione[1] (quando il prodotto è contrassegnato)	**Valore**
c-UL-us	Omologazione UL per Classe I, Divisione 2, Gruppi A,B,C,D, aree pericolose, certificazione per U.S.A. e Canada. Vedere File UL E194810
CE	Direttiva EMC 2004/108/EEC dell'Unione Europea, conformità con: • EN 61000-6-4; emissioni industriali • EN 61131-2; controllori programmabili (Articolo 8, Zone A e B) • EN 61326-1; requisiti industriali di Misur./Controllo/Lab. • EN 61000-6-2; immunità industriale
C-Tick	Australian Radiocommunications Act, conformità con: AS/NZS CISPR 11; emissioni industriali
TÜV	Certificazione TÜV per la sicurezza funzionale Sicurezza funzionale: SIL 1 ... 3, conformemente a IEC 61508; livello prestazionale PL(e) conformemente a ISO 13849-1, Categoria 1 ... 4, conformemente a EN954-1; NFPA79
UL	Certificazione UL per la sicurezza funzionale. Vedere UL File E256621
ODVA	Conformità ODVA collaudata in base alle specifiche DeviceNet e Ethernet/IP

(1) Vedere il collegamento "Certificazioni dei prodotti" all'indirizzo http://ab.com per dichiarazioni di conformità, certificati ed altri dettagli di certificazione.

Note:

Indicatori di stato

Introduzione

Argomento	Pagina
Indicatori di stato del modulo	201
Identificazione degli errori tramite gli indicatori di stato del modulo ed il display alfanumerico	206
Identificazione degli errori EtherNet/IP tramite gli indicatori di stato ed il display alfanumerico	210

Indicatori di stato del modulo

Fare riferimento a queste tabelle per interpretare il colore degli indicatori di stato ed adottare le azioni consigliate dove applicabile.

ATTENZIONE

Gli indicatori di stato non sono indicatori affidabili per le funzioni di sicurezza. Devono essere utilizzati solo per una diagnostica generale nella messa in servizio e ricerca guasti. Non utilizzare gli indicatori di stato come indicatori funzionali.

Descrizione degli indicatori di stato del modulo (MS)

Indicatore di stato del modulo (MS)	Significato	Azione da intraprendere
Spento	Alimentazione assente	Vedere la procedura riportata sotto questa tabella.
Verde, acceso	Il controllore funziona in modalità RUN e presenta condizioni normali.	Nessuna azione richiesta.
Verde, lampeggiante	Il controllore è in modalità di riposo.	
Rosso, lampeggiante	Errore reversibile.	Vedere la procedura riportata sotto questa tabella.
Rosso, acceso	Errore irreversibile.	
Rosso/verde, lampeggiante	Autotest in corso. Oppure la configurazione del controllore viene scaricata, è incompleta o errata. Ad esempio, l'ID rete (UNID) non è impostato.	

Se l'indicatore di stato del modulo è spento, procedere come segue.

1. Spegnere e riaccendere l'alimentatore.
2. Intraprendere azioni correttive per il disturbo.
3. Contattare Rockwell Automation.

Se l'indicatore di stato del modulo è rosso lampeggiante, procedere come segue.

1. Configurare correttamente i selettori.

2. Ripristinare i dati di configurazione.

Se l'indicatore di stato del modulo è rosso fisso (acceso), procedere come segue.

1. Spegnere e riaccendere l'alimentatore.
2. Verificare il cablaggio esterno.
3. Intraprendere azioni correttive per il disturbo.
4. Contattare Rockwell Automation.

Se l'indicatore di stato del modulo è rosso e verde lampeggiante, procedere come segue.

1. Configurare correttamente i selettori.
2. Impostare il numero rete di sicurezza
3. Riconfigurare il dispositivo.

Descrizione degli indicatori di stato della rete DeviceNet (NS D)

Indicatore di stato della rete DeviceNet (NS D)	Significato	Azione da intraprendere
Spento	Il controllore non è online oppure non viene alimentato dalla rete DeviceNet.	Vedere la procedura riportata sotto questa tabella.
Verde, acceso	Il controllore è online; il collegamento è stato stabilito.	Nessuna azione richiesta.
Verde, lampeggiante	Il controllore è online; non è stato stabilito alcun collegamento.	
Rosso, acceso	Errore di comunicazione dovuto a un ID MAC duplicato (codice di errore F0) o a un bus disattivato (codice di errore F1).	Vedere la procedura riportata sotto questa tabella.
Rosso, lampeggiante	Timeout della comunicazione.	
Rosso/verde, lampeggiante	Impostazione in corso del numero rete di sicurezza (SNN).	Nessuna azione richiesta.

Se l'indicatore di stato della rete è spento, procedere come segue.

1. Spegnere e riaccendere l'alimentatore.
2. Verificare il cablaggio esterno.
3. Intraprendere azioni correttive per il disturbo.
4. Contattare Rockwell Automation.

Se l'indicatore di stato della rete è rosso acceso o lampeggiante, procedere come segue.

1. Visualizzare il display alfanumerico per conoscere l'indirizzo di nodo dell'errore e il codice di errore.
2. Verificare che l'indirizzo di nodo non sia stato duplicato.

3. Verificare che la velocità di comunicazione sia identica per tutti i nodi.
4. Verificare che i cavi non siano allentati, scollegati o troppo lunghi.
5. Verificare che i resistori di terminazione siano stati installati solo su entrambe le estremità della linea principale.
6. Intraprendere azioni correttive per il disturbo.
7. Accertarsi che i dispositivi di destinazione siano configurati, verificati e in uno stato operativo normale.

Descrizione degli indicatori di stato di blocco configurazione (blocco)

Indicatore di blocco configurazione (blocco)	Significato	Azione da intraprendere
Giallo, acceso	Esiste una configurazione valida bloccata.	Nessuna azione richiesta.
Giallo, lampeggiante	Esiste una configurazione valida non bloccata.	Bloccare la configurazione prima di utilizzare il sistema di sicurezza.
Spento	La configurazione non è valida.	Riconfigurare il controllore.

Descrizione degli indicatori di stato della comunicazione USB (Comm U)

Indicatore di stato comunicazione USB (Comm U)	Significato	Azione da intraprendere
Giallo, lampeggiante	Comunicazione del controllore in corso.	Nessuna azione richiesta.
Spento	Assenza di comunicazione del controllore.	

Descrizione degli indicatori di stato degli I/O (ingressi 0...15, uscite 0...7)

Indicatore di stato I/O	Significato	Azione da intraprendere
Rosso, acceso	È stato rilevato un errore nel circuito elettrico di ingresso o di uscita oppure si è verificato un errore di discrepanza nell'I/O impostato per la modalità a doppio canale.	Vedere la procedura riportata sotto questa tabella.
Rosso, lampeggiante	È stato rilevato un errore nella configurazione del canale duale del circuito I/O associato.	
Spento	Il segnale di ingresso o di uscita è disattivato.	
Giallo, acceso	Il segnale di ingresso o di uscita è attivato.	Nessuna azione richiesta.

Se l'indicatore di stato I/O è acceso o rosso lampeggiante, procedere come segue.

1. Verificare che il cavo del segnale:

– non sia a contatto con la sorgente di alimentazione (polo positivo)
– non presenti un guasto verso terra
– non sia scollegato.

2. Verificare l'assenza di cortocircuito tra i cavi di segnale.

3. Verificare l'assenza di sovracorrente per l'uscita.
4. Verificare l'assenza di guasti nei dispositivi collegati.
5. Verificare che le impostazioni del tempo di discrepanza siano valide.

Se l'indicatore di stato I/O è spento, procedere come segue.

1. Verificare che la tensione di alimentazione impostata rientri nell'intervallo specificato.
2. Verificare che tutti i cavi siano collegati.

Descrizione degli indicatori di stato della rete EtherNet/IP (NS E)

Indicatore di stato EtherNet/IP (NS E)	Significato	Azione da intraprendere
Spento	Il controllore non ha un indirizzo IP o non è acceso.	Vedere la procedura riportata sotto questa tabella.
Verde, lampeggiante	Il controllore non ha connessioni stabilite ma ha un indirizzo IP.	
Verde, acceso	Il controllore ha almeno una connessione stabilita (anche al router dei messaggi).	Nessuna azione richiesta.
Rosso, lampeggiante	Una o più connessioni per questo dispositivo target è in timeout. Questo stato terminerà solo se tutte le connessioni in timeout vengono ristabilite o se il dispositivo viene ripristinato.	Vedere la procedura riportata sotto questa tabella.
Rosso, acceso	Il controllore ha rilevato che il suo indirizzo IP è già in uso.	Reset dell'indirizzo IP.

Se l'indicatore di stato EtherNet/IP è spento, procedere come segue.

1. Alimentare il controllore.
2. Impostare l'indirizzo IP.

Se l'indicatore di stato EtherNet/IP è verde lampeggiante, procedere come segue.

1. Controllare il cablaggio del controllore.
2. Configurare l'origine per la connessione al target.

Se l'indicatore di stato EtherNet/IP è rosso lampeggiante, procedere come segue.

1. Verificare il cablaggio esterno.
2. Controllare i punti terminali.
3. Controllare gli interruttori.

Descrizione degli indicatori di stato della comunicazione EtherNet/IP (COMM E)

Indicatore di stato comunicazione (COMM E)	Significato	Azione da intraprendere
Verde, acceso	Il controllore comunica sulla rete Ethernet.	Nessuna azione richiesta.
Spento	Il controllore non comunica sulla rete Ethernet.	

Descrizione degli indicatori di stato della velocità della rete Ethernet (100)

Indicatore di stato velocità rete (100)	Significato	Azione da intraprendere
Giallo, acceso	La velocità di comunicazione è 100 Mbps.	Nessuna azione richiesta.
Spento[1]	La velocità di comunicazione è 10 Mbps.	Controllare che l'indicatore della velocità della rete (10) sia acceso.

(1) Se questo indicatore è spento insieme all'indicatore della velocità della rete (10), controllare la connessione Ethernet.

Descrizione degli indicatori della velocità della rete Ethernet (10)

Indicatore di stato velocità rete (10)	Significato	Azione da intraprendere
Giallo, acceso	La velocità di comunicazione è 10 Mbps.	Nessuna azione richiesta.
Spento[1]	La velocità di comunicazione è 100 Mbps.	Controllare che l'indicatore della velocità della rete (100) sia acceso.

(1) Se questo indicatore è spento insieme all'indicatore della velocità della rete (10), controllare la connessione Ethernet.

Identificazione degli errori tramite gli indicatori di stato del modulo ed il display alfanumerico

Utilizzare le tabelle seguenti per interpretare le combinazioni di colore e stato degli indicatori di stato e degli indicatori del display alfanumerico e intraprendere le azioni correttive, se possibile.

Errori critici

Indicatori			Registro errori	Causa	Azione correttiva
MS	**NS**	**Codice display alfanumerico**			
Spento	Spento	Spento	Nessuno	Errore hardware critico. Livello di disturbo superiore a quello previsto.	1. Spegnere e riaccendere l'alimentatore. 2. Verificare il cablaggio esterno. 3. Intraprendere azioni correttive per il disturbo. 4. Contattare Rockwell Automation.
Rosso, acceso	Spento	Sinistra: H Destra: ---	Guasto del sistema	Errore hardware critico. Livello di disturbo superiore a quello previsto. Morsetto di uscita in corto a 24V CC prima del funzionamento.	
Rosso, acceso	Spento	P6	Guasto del sistema	Morsetto di uscita in corto a 24V CC prima del funzionamento.	1. Spegnere e riaccendere l'alimentatore. 2. Verificare il cablaggio esterno.

Errore di interruzione

Indicatori			Registro errori	Causa	Azione correttiva
MS	**NS**	**Codice display alfanumerico(1)**			
Rosso, lampeggiante	Verde, acceso o lampeggiante	E8	Non corrispondenza dell'impostazione dei selettori	L'indirizzo di nodo e la velocità di trasmissione sono stati modificati dopo il normale completamento del download della configurazione.	1. Impostare correttamente i selettori. 2. Riconfigurare il dispositivo.

(1) Sul display vengono visualizzati alternativamente il codice di errore e l'indirizzo di nodo dell'errore.

Errori reversibili

Indicatori			Registro errori	Causa	Azione correttiva
MS	**Codice display alfanumerico(1)**	**I/O**			
Rosso, acceso	F0	---	Duplicate MAC ID	È stato impostato lo stesso indirizzo di nodo per più nodi.	Verificare che gli indirizzi di nodo non siano stati duplicati e riconfigurare il dispositivo, se necessario.

Errori reversibili

Indicatori			Registro errori	Causa	Azione correttiva
MS	**Codice display alfanumerico(1)**	**I/O**			
Rosso, acceso	F1	---	Bus Off	La comunicazione viene interrotta a causa dei frequenti errori nei dati.	1. Verificare che la velocità di comunicazione sia identica per tutti i nodi. 2. Verificare che i cavi non siano allentati, scollegati o troppo lunghi. 3. Verificare che i resistori di terminazione siano stati installati solo su entrambe le estremità della linea principale. 4. Intraprendere azioni correttive per il disturbo. 5. Spegnere e riaccendere l'alimentatore.
Rosso, lampeggiante	L9	---	Standard I/O Connection Timeout	Timeout di collegamento I/O standard.	
Rosso, lampeggiante	dA	---	Safety I/O Connection Timeout	Timeout di collegamento I/O di sicurezza.	
Rosso, lampeggiante	d5	---	Nonexistent Slave Device	Nessuno slave rilevato.	
Rosso, lampeggiante	d6	---	Safety I/O Connection Establishment Failure	Impossibile stabilire il collegamento I/O di sicurezza.	Verificare che il dispositivo slave sia configurato e che funzioni normalmente.
Rosso, lampeggiante	d6	---	Invalid Slave Device	Dispositivo slave non valido a causa di un errore di verifica.	1. Verificare la configurazione del dispositivo slave. 2. Collegare un dispositivo slave compatibile.
Spento	E0	---	Network PS Voltage Low	La tensione dell'alimentatore di rete è bassa.	1. Verificare che la tensione di alimentazione impostata rientri nell'intervallo specificato. 2. Verificare che i cavi non siano allentati o scollegati.
---	E2	---	Transmission Timeout	Timeout di trasmissione DeviceNet o assenza di collegamenti alla rete DeviceNet.	1. Verificare che la velocità di comunicazione sia identica per tutti i nodi. 2. Verificare che i cavi non siano allentati, scollegati o troppo lunghi. 3. Verificare che i resistori di terminazione siano stati installati solo su entrambe le estremità della linea principale. 4. Intraprendere azioni correttive per il disturbo.
Rosso, lampeggiante	A0	---	Comunicazione I/O di sicurezza relativa interrotta in seguito a un errore di comunicazione I/O di sicurezza	Un timeout del collegamento I/O di sicurezza ha determinato l'interruzione della relativa connessione I/O di sicurezza.	
Rosso, lampeggiante	A1	---	Comunicazione I/O di sicurezza completamente interrotta in seguito a un errore di comunicazione I/O di sicurezza	Un timeout del collegamento I/O di sicurezza ha determinato l'interruzione di tutti i collegamenti I/O.	
---	P4	Tutti OFF	Input PS Voltage Low	L'alimentazione I/O per gli ingressi (V1, G1) non è collegata, sebbene venga utilizzato un morsetto di ingresso di sicurezza o un morsetto dell'uscita di test.	1. Verificare che la tensione di alimentazione impostata rientri nell'intervallo specificato. 2. Verificare che i cavi non siano allentati o scollegati.
---	P5	Tutti OFF	Output PS Voltage Low	L'alimentazione I/O per le uscite (V2, G2) non è collegata, sebbene venga utilizzato un morsetto di uscita di sicurezza.	

Errori reversibili

Indicatori			Registro errori	Causa	Azione correttiva
MS	**Codice display alfanumerico(1)**	**I/O**			
---	P1	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	External Test Signal Failure at Safety Input	Si è verificato un errore di cablaggio esterno per un ingresso di sicurezza.	1. Verificare che il cavo del segnale: • non sia a contatto con la sorgente di alimentazione (polo positivo) • non presenti un guasto verso terra • non sia scollegato. 2. Verificare l'assenza di cortocircuito tra i cavi di segnale. 3. Verificare l'assenza di guasti nei dispositivi collegati. 4. Verificare che le impostazioni del tempo di discrepanza siano valide. Per il ripristino da questo stato di errore, è necessario che il tempo di mantenimento dello stato di errore dell'ingresso sia trascorso e che la causa dell'errore sia stata eliminata. Gli ingressi di sicurezza di destinazione devono essere disattivati. Per modificare il tempo di discrepanza, è necessario riconfigurare l'ingresso di sicurezza.
---	P1	Morsetto di destinazione rosso, acceso	Discrepancy Error at Safety Input	Si è verificato un errore di discrepanza tra due ingressi configurati per il canale duale.	
---	P1	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	Internal Input Failure at Safety Input	Si è verificato un errore del circuito interno per l'ingresso di sicurezza.	
---	P2	N/D	Overload Detected at Test Output	È stato rilevato un sovraccarico nell'uscita di test, quando un'uscita di test è stata configurata come uscita di segnale standard.	Verificare se il cavo del segnale di uscita presenta un guasto verso terra o se è sovraccarico.
---	P2	N/D	Stuck-at-high Detected at Test Output	Un'uscita di test, configurata come uscita di segnale standard, è bloccata nello stato on.	1. Verificare che la fonte di alimentazione (polo positivo) non sia a contatto con il cavo del segnale di uscita. Una volta trascorso il tempo di mantenimento dello stato di errore dell'ingresso e dopo aver eliminato la causa dell'errore, disattivare l'ingresso. L'errore verrà ripristinato. 2. Se i cavi non presentano alcun problema, sostituire l'unità.
---	P2	N/D	Rilevata sottocorrente per la spia di muting	Rilevamento della disconnessione della spia nell'uscita di test, quando il morsetto T3 è configurato come uscita di segnale spia di muting.	1. Verificare che il cavo del segnale di uscita non sia scollegato. 2. Controllare la spia per accertarsi che funzioni.

Errori reversibili

Indicatori			Registro errori	Causa	Azione correttiva
MS	**Codice display alfanumerico[1]**	**I/O**			
---	P3	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	Sovracorrente rilevata per l'uscita di sicurezza	È stata rilevata una sovracorrente nell'uscita di sicurezza.	1. Verificare l'assenza di sovracorrente per l'uscita. 2. Verificare che il cavo del segnale: • non sia a contatto con la sorgente di alimentazione (polo positivo) • non presenti un guasto verso terra 3. Verificare l'assenza di cortocircuito tra i cavi di segnale. Per il ripristino da questo stato di errore, è necessario che il tempo di mantenimento dello stato di errore dell'ingresso sia trascorso e che la causa dell'errore sia stata eliminata. Il segnale di uscita proveniente dall'applicazione utente per l'uscita di sicurezza di destinazione deve essere disattivato.
---	P3	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	Rilevato cortocircuito nell'uscita di sicurezza	È stato rilevato un cortocircuito nell'uscita di sicurezza.	
---	P3	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	Stuck-at-high Detected at Safety Output	Un'uscita di sicurezza è bloccata in stato on.	
---	P3	Morsetto di destinazione rosso, acceso Morsetto accoppiato rosso, lampeggiante	Cross Connection Detected at Safety Output	È stato rilevato un collegamento incrociato nell'uscita di sicurezza.	
---	P3	Morsetto di destinazione rosso, acceso	Dual Channel Violation at Safety Output	Si è verificato un errore di dati di uscita nell'uscita di sicurezza. Ad esempio, un'uscita è configurata come canale duale, ma solo uno dei bit di uscita viene attivato dal programma.	Verificare che i dati di uscita del programma per due uscite nella modalità Canale duale siano configurati come canali equivalenti.

(1) Sul display vengono visualizzati alternativamente il codice di errore e l'indirizzo di nodo dell'errore.

Identificazione degli errori EtherNet/IP tramite gli indicatori di stato ed il display alfanumerico

Utilizzare le tabelle seguenti per interpretare le combinazioni di colore e stato degli indicatori di stato e degli indicatori del display alfanumerico e intraprendere le azioni correttive, se possibile.

Per il controllore 1752-L24BBBE, quando si preme il pulsante di visualizzazione dell'indirizzo IP per almeno 1 secondo, il display visualizza l'indirizzo EtherNet/IP impostato. Se si verifica un errore nella configurazione EtherNet/IP, viene visualizzato il codice di errore "n4".

Errori del controllore EtherNet/IP

Indicatori			Registro errori	Causa	Azione correttiva
MS	**NS**	**Codice display alfanumerico[1]**			
Spento	Rosso, acceso	UF	Guasto del sistema	Guasto hardware di un adattatore EtherNet/IP.	Spegnere e riaccendere l'alimentatore. Se il guasto persiste, sostituire il controllore.
Rosso, acceso	---	F0		Errore di duplicazione di un indirizzo IP.	Controllare l'indirizzo IP degli altri dispositivi ed impostare un indirizzo che non sia uguale a nessun altro.
Spento	---	E3		Errore di connessione del server BOOTP.	1. Verificare che il cavo sia collegato correttamente. 2. Verificare che il server BOOTP funzioni normalmente.
Spento	---	F2		Errore di elaborazione logica delle impostazioni di base.	Controllare la configurazione. Se il guasto persiste, sostituire il controllore.
Spento	Rosso, lampeggiante	E9		Errore di memoria EtherNet/IP.	Spegnere e riaccendere l'alimentatore. Se il guasto persiste, sostituire il controllore.
Spento	Rosso, lampeggiante	F4		Errore del controllore di comunicazione EtherNet/IP.	
Rosso, lampeggiante	---	L9		Errore di comunicazione target standard EtherNet/IP.	1. Verificare che ogni nodo usi le stesse impostazioni di comunicazione 2. Verificare che i cavi non siano scollegati o piegati. 3. Verificare che l'origine sia alimentata.
Spento	---	E1		Errore di collegamento Off.	1. Verificare che ogni nodo usi le stesse impostazioni di comunicazione 2. Verificare che i cavi non siano scollegati o piegati. 3. Verificare che l'hub sia alimentato.

(1) Il display visualizza in modo alternato il codice di errore e n4.

Riferimento per i comandi delle funzioni logiche

Introduzione

Nella presente appendice vengono descritte le funzioni logiche utilizzate per la programmazione.

Argomento	Pagina
Istruzione NOT	211
Istruzione AND	212
Istruzione OR	214
Istruzione Exclusive OR	216
Istruzione Exclusive NOR	217
Istruzione Routing	218
Istruzione Reset Set Flip-flop (RS-FF)	218
Istruzione Multi-connector	219
Istruzione Comparator	220

Istruzione NOT

Restituisce il valore negato di quello di ingresso.

Diagramma dell'istruzione NOT

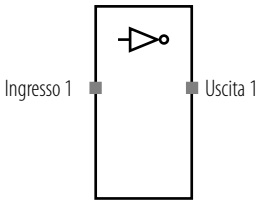


Tabella verità dell'istruzione NOT

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Ingresso 1	Uscita 1
0	1
1	0

Istruzione AND

L'uscita è un AND logico di massimo otto condizioni di ingresso. È possibile impostare il numero di ingressi utilizzando la scheda In/Out Setting della finestra di dialogo Function Block Properties. L'impostazione di default è due ingressi.

Diagramma dell'istruzione AND

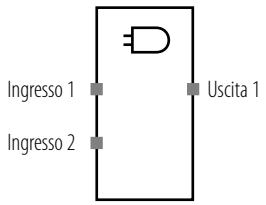


Tabelle verità dell'istruzione AND

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato. La lettera x minuscola indica un valore indifferente.

Tabella verità per la valutazione AND a un ingresso

Ingresso 1	Uscita 1
0	0
1	1

Tabella verità per la valutazione AND a due ingressi

Ingresso 1	Ingresso 2	Uscita 1
0	x	0
x	0	0
1	1	1

Tabella verità per la valutazione AND a tre ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Uscita 1
0	x	x	0
x	0	x	0
x	x	0	0
1	1	1	1

Tabella verità per la valutazione AND a quattro ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Uscita 1
0	x	x	x	0
x	0	x	x	0
x	x	0	x	0
x	x	x	0	0
1	1	1	1	1

Tabella verità per la valutazione AND a cinque ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Uscita 1
0	x	x	x	x	0
x	0	x	x	x	0
x	x	0	x	x	0
x	x	x	0	x	0
x	x	x	x	0	0
1	1	1	1	1	1

Tabella verità per la valutazione AND a sei ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Uscita 1
0	x	x	x	x	x	0
x	0	x	x	x	x	0
x	x	0	x	x	x	0
x	x	x	0	x	x	0
x	x	x	x	0	x	0
x	x	x	x	x	0	0
1	1	1	1	1	1	1

Tabella verità per la valutazione AND a sette ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Ingresso 7	Uscita 1
0	x	x	x	x	x	x	0
x	0	x	x	x	x	x	0
x	x	0	x	x	x	x	0
x	x	x	0	x	x	x	0
x	x	x	x	0	x	x	0
x	x	x	x	x	0	x	0
x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1

Tabella verità per la valutazione AND a otto ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Ingresso 7	Ingresso 8	Uscita 1
0	x	x	x	x	x	x	x	0
x	0	x	x	x	x	x	x	0
x	x	0	x	x	x	x	x	0
x	x	x	0	x	x	x	x	0
x	x	x	x	0	x	x	x	0
x	x	x	x	x	0	x	x	0
x	x	x	x	x	x	0	x	0
x	x	x	x	x	x	x	0	0
1	1	1	1	1	1	1	1	1

Istruzione OR

L'uscita è un OR logico di massimo otto condizioni di ingresso. È possibile impostare il numero di ingressi utilizzando la scheda In/Out Setting della finestra di dialogo Function Block Properties. L'impostazione di default è due ingressi.

Diagramma dell'istruzione OR

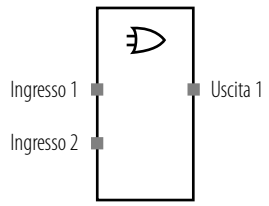


Tabelle verità dell'istruzione OR

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato. La lettera x minuscola indica un valore indifferente.

Tabella verità per la valutazione OR a un ingresso

Ingresso 1	Uscita 1
0	0
1	1

Tabella verità per la valutazione OR a due ingressi

Ingresso 1	Ingresso 2	Uscita 1
0	0	0
1	x	1
x	1	1

Tabella verità per la valutazione OR a tre ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Uscita 1
0	0	0	0
1	x	x	1
x	1	x	1
x	x	1	1

Tabella verità per la valutazione OR a quattro ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Uscita 1
0	0	0	0	0
1	x	x	x	1
x	1	x	x	1
x	x	1	x	1
x	x	x	1	1

Tabella verità per la valutazione OR a cinque ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Uscita 1
0	0	0	0	0	0
1	x	x	x	x	1
x	1	x	x	x	1
x	x	1	x	x	1
x	x	x	1	x	1
x	x	x	x	1	1

Tabella verità per la valutazione OR a sei ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Uscita 1
0	0	0	0	0	0	0
1	x	x	x	x	x	1
x	1	x	x	x	x	1
x	x	1	x	x	x	1
x	x	x	1	x	x	1
x	x	x	x	1	x	1
x	x	x	x	x	1	1

Tabella verità per la valutazione OR a sette ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Ingresso 7	Uscita 1
0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	1
x	1	x	x	x	x	x	1
x	x	1	x	x	x	x	1
x	x	x	1	x	x	x	1
x	x	x	x	1	x	x	1
x	x	x	x	x	1	x	1
x	x	x	x	x	x	1	1

Tabella verità per la valutazione OR a otto ingressi

Ingresso 1	Ingresso 2	Ingresso 3	Ingresso 4	Ingresso 5	Ingresso 6	Ingresso 7	Ingresso 8	Uscita 1
0	0	0	0	0	0	0	0	0
1	x	x	x	x	x	x	x	1
x	1	x	x	x	x	x	x	1
x	x	1	x	x	x	x	x	1
x	x	x	1	x	x	x	x	1
x	x	x	x	1	x	x	x	1
x	x	x	x	x	1	x	x	x
x	x	x	x	x	x	1	x	1
x	x	x	x	x	x	x	1	1

Istruzione Exclusive OR

L'uscita è un OR esclusivo delle condizioni di ingresso.

Diagramma dell'istruzione Exclusive OR

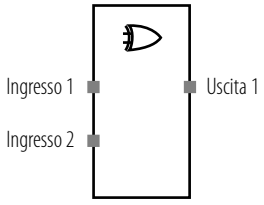


Tabella verità dell'istruzione Exclusive OR

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per la valutazione di Exclusive OR

Ingresso 1	Ingresso 2	Uscita 1
0	0	0
0	1	1
1	0	1
1	1	0

Istruzione Exclusive NOR

L'uscita è un NOR esclusivo delle condizioni di ingresso.

Diagramma dell'istruzione Exclusive NOR

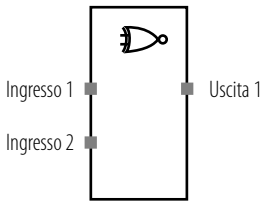


Tabelle verità dell'istruzione Exclusive NOR

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per la valutazione Exclusive NOR

Ingresso 1	Ingresso 2	Uscita 1
0	0	1
0	1	0
1	0	0
1	1	1

Istruzione Routing

L'istruzione Routing conduce un segnale di ingresso a un massimo di otto segnali di uscita. Viene utilizzata per inviare un segnale a più indirizzi fisici, ad esempio un tag di uscita. È possibile impostare il numero di uscite utilizzando la scheda I/O Setting della finestra di dialogo Function Block Properties. L'impostazione di default è 1.

Diagramma dell'istruzione Routing

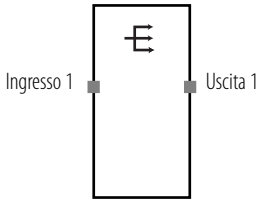


Tabella verità dell'istruzione Routing

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per la valutazione dell'istruzione Routing

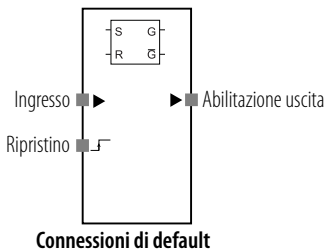
Ingresso 1	Uscita 1	Uscita 2	Uscita 3	Uscita 4	Uscita 5	Uscita 6	Uscita 7	Uscita 8
0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1

Istruzione Reset Set Flip-flop (RS-FF)

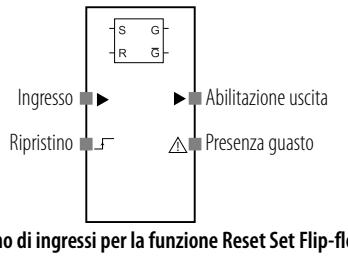
Quando il segnale di ingresso è attivo, il segnale di abilitazione uscita viene attivato. Il segnale di abilitazione uscita resta attivo anche se il segnale di ingresso viene disattivato. Quando il segnale di ripristino è attivo, il segnale di abilitazione uscita viene disattivato.

Nella programmazione è possibile utilizzare anche l'uscita opzionale Fault Present. Per abilitarla, selezionare la casella di controllo Use Fault Present nella scheda I/O Settings della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet.

Diagramma dell'istruzione Reset Set Flip-flop



Connessioni di default



N. massimo di ingressi per la funzione Reset Set Flip-flop

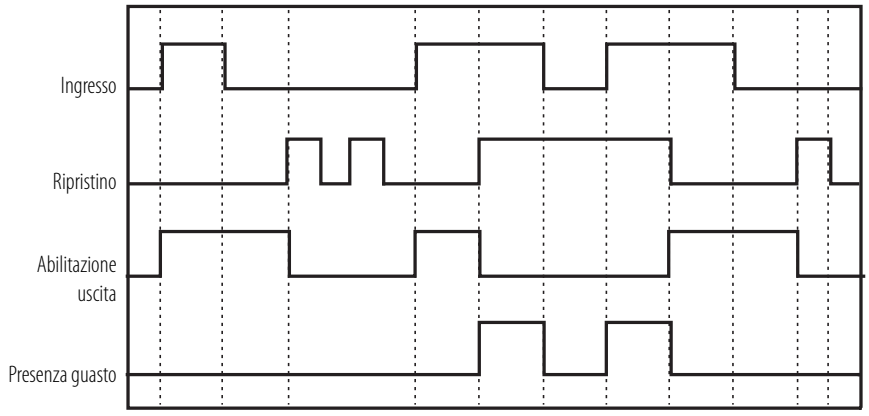
Gestione degli errori dell'istruzione Reset Set Flip-flop

Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nell'istruzione RS Flip-flop.

Rilevamento errori e ripristino per l'istruzione Reset Set Flip-flop

Condizione di errore	Stato al verificarsi dell'errore		Per ripristinare la condizione di errore
	Abilitazione uscita	Presenza guasto	
L'ingresso e il ripristino sono attivi simultaneamente	OFF (Stato di sicurezza)	ON	Disattivare uno dei segnali.

Diagramma dei tempi dell'istruzione Reset Set Flip-flop

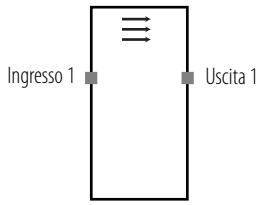


Istruzione Multi-connector

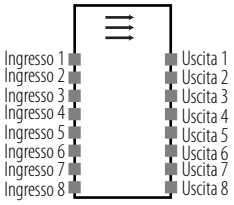
L'istruzione Multi-connector converte i segnali di ingresso (otto ingressi massimo) in segnali di uscita (otto uscite massimo). I segnali di ingresso e i segnali di uscita sono associati uno a uno per i segnali da uno a otto. Lo stato degli altri segnali di ingresso è indifferente.

È possibile portare il numero di ingressi e di uscite a otto nella scheda I/O Settings della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet. L'impostazione di default è 1.

Diagramma dell'istruzione Multi-connector



Connessioni di default



N. massimo di I/O per l'istruzione Multi-connector

Tabella verità per l'istruzione Multi-connector

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

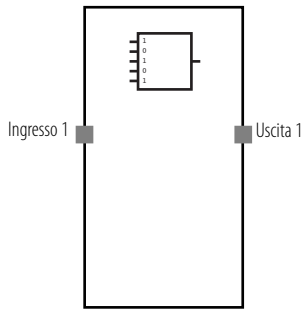
Tabella verità per l'istruzione Multi-connector

Ingressi								Uscite							
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0	x	x	x	x	x	x	x	0	x	x	x	x	x	x	x
1	x	x	x	x	x	x	x	1	x	x	x	x	x	x	x
x	0	x	x	x	x	x	x	x	0	x	x	x	x	x	x
x	1	x	x	x	x	x	x	x	1	x	x	x	x	x	x
x	x	0	x	x	x	x	x	x	x	0	x	x	x	x	x
x	x	1	x	x	x	x	x	x	x	1	x	x	x	x	x
x	x	x	0	x	x	x	x	x	x	x	0	x	x	x	x
x	x	x	1	x	x	x	x	x	x	x	1	x	x	x	x
x	x	x	x	0	x	x	x	x	x	x	x	0	x	x	x
x	x	x	x	1	x	x	x	x	x	x	x	1	x	x	x
x	x	x	x	x	0	x	x	x	x	x	x	x	0	x	x
x	x	x	x	x	1	x	x	x	x	x	x	x	1	x	x
x	x	x	x	x	x	0	x	x	x	x	x	x	x	0	x
x	x	x	x	x	x	1	x	x	x	x	x	x	x	1	x
x	x	x	x	x	x	x	0	x	x	x	x	x	x	x	0
x	x	x	x	x	x	x	1	x	x	x	x	x	x	x	1

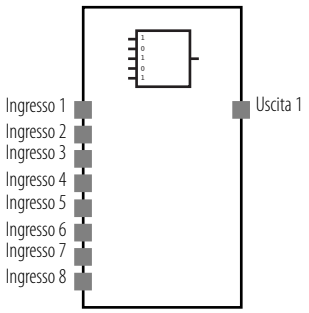
Istruzione Comparator

L'istruzione Comparator confronta i segnali di ingresso specificati di massimo otto ingressi con il modello di comparazione configurato e attiva il segnale di uscita 1 se tutti i segnali di ingresso corrispondono al modello di comparazione. Il segnale di uscita 1 viene disattivato quando i segnali di ingresso non corrispondono più al valore di confronto.

Diagramma dell'istruzione Comparator



Connessioni di default



N. massimo di I/O per l'istruzione Comparator

Parametri dell'istruzione Comparator

Impostare i seguenti parametri per l'istruzione Comparator.

Parametri del blocco funzione Comparator

Parametro	Opzioni valide	Impostazione di default
Valore di comparazione	00000000-11111111 (bit 7-0)	00000001

È possibile impostare il modello di comparazione e portare il numero di ingressi da uno a otto nella scheda In/Out Setting della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet. L'impostazione di default è un ingresso. Il modello di comparazione viene impostato utilizzando una combinazione di 0 (ingresso disattivato), 1 (ingresso attivato) e X (ingresso attivato o disattivato).

Tabella verità per l'istruzione Comparator

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato. VC è il valore di confronto. Una X indica che lo stato dell'ingresso (corrispondente o meno) non è applicabile.

Tabella verità per l'istruzione Comparator

Ingresso 8	Ingresso 7	Ingresso 6	Ingresso 5	Ingresso 4	Ingresso 3	Ingresso 2	Ingresso 1	Uscita 1
≠VC per bit 7	X	X	X	X	X	X	X	0
X	≠VC per bit 6	X	X	X	X	X	X	0
X	X	≠VC per bit 5	X	X	X	X	X	0
X	X	X	≠VC per bit 4	X	X	X	X	0
X	X	X	X	≠VC per bit 3	X	X	X	0
X	X	X	X	X	≠VC per bit 2	X	X	0
X	X	X	X	X	X	≠VC per bit 1	X	0
X	X	X	X	X	X	X	≠VC per bit 0	0
= VC per bit 7	= VC per bit 6	= VC per bit 5	= VC per bit 4	= VC per bit 3	= VC per bit 2	= VC per bit 1	= VC per bit 0	1

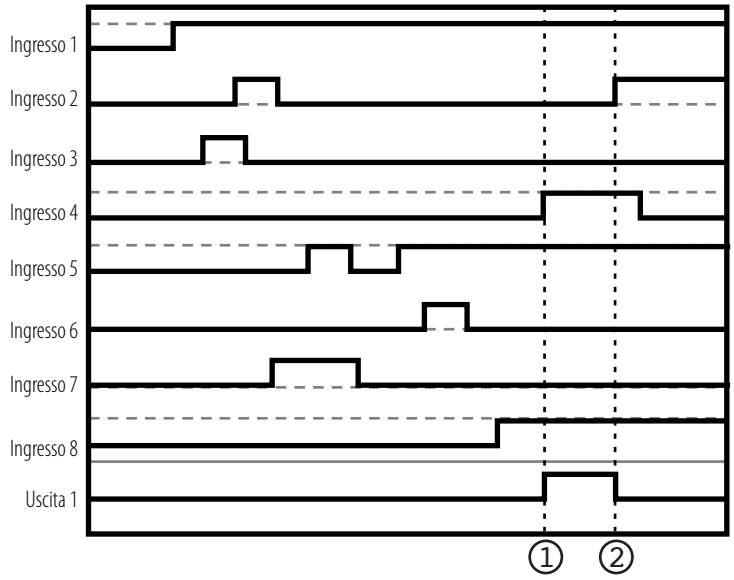
Diagramma dei tempi dell'istruzione Comparator

Le linee orizzontali tratteggiate nel diagramma rappresentano i valori di confronto (VC) per ogni ingresso.

1. L'uscita 1 viene attivata se tutti i segnali di ingresso corrispondono al valore di confronto.

2. Il segnale di uscita 1 viene disattivato se uno dei segnali di ingresso non corrisponde al valore di confronto.

Diagramma dei tempi dell'istruzione Comparator



Note:

Riferimento per i comandi dei blocchi funzione

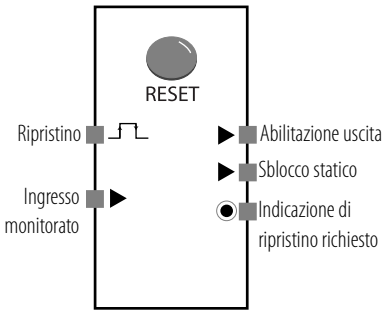
Introduzione

Nella presente appendice vengono descritti i blocchi funzione utilizzati per la programmazione.

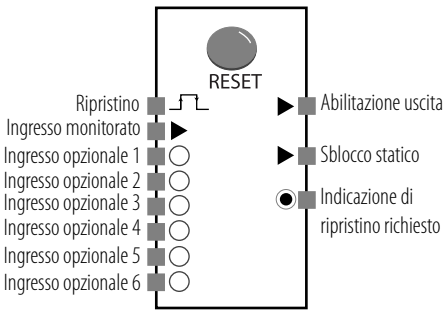
Argomento	Pagina
Blocco funzione Reset	225
Blocco funzione Restart	227
Emergency Stop (ESTOP)	229
Blocco funzione LC (Light Curtain)	232
Blocco funzione Safety Gate Monitoring	234
Blocco funzione Two-hand Control	239
Blocco funzione OFF-delay Timer	242
Blocco funzione ON-delay Timer	242
Blocco funzione User Mode Switch	243
EDM (External Device Monitoring)	245
Muting	247
Enable switch	264
Pulse Generator	267
Counter	268

Blocco funzione Reset

Diagramma del blocco funzione Reset



Connessioni di default



N. massimo di ingressi per la funzione Reset

È possibile portare il numero di ingressi da due a otto nella scheda I/O Settings della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet. Il numero di ingressi di default è due.

Il segnale di abilitazione uscita viene attivato se il segnale di ripristino viene ricevuto correttamente quando la condizione Ingresso monitorato del blocco funzione Reset è attiva. Questo blocco funzione può essere utilizzato per impedire che la macchina venga ripristinata automaticamente all'accensione del controllore, quando la modalità operativa viene modificata da riposo a RUN o quando viene attivato un segnale proveniente da un dispositivo di ingresso di sicurezza.

Le uscite Sblocco statico e Indicazione di ripristino richiesto sono opzionali. Per abilitarle, selezionare la casella di controllo corrispondente nella scheda Out point della finestra di dialogo Function Block Properties.

Condizioni di attivazione delle uscite

Uscita	Condizione di attivazione
Abilitazione uscita	L'ingresso monitorato e tutti gli ingressi opzionali abilitati devono essere attivati ed è necessario che il segnale di ripristino venga ricevuto correttamente.
Sblocco statico	L'ingresso monitorato e tutti gli ingressi opzionali abilitati devono essere attivati.
Indicazione di ripristino richiesto	L'Indicazione di ripristino richiesto diventa un'uscita ad impulsi a 1 Hz se l'ingresso monitorato e tutti gli ingressi opzionali abilitati sono attivati e il segnale di abilitazione uscita è disattivato. L'Indicazione di ripristino richiesto viene attivata solo quando il segnale di ripristino è attivato.

Parametri del blocco funzione Reset

È possibile impostare il segnale di ripristino su Low-High-Low o su Rising Edge utilizzando la scheda Parameter della finestra di dialogo Function Block Properties. L'impostazione di default è Low-High-Low.

Con la configurazione Low-High-Low, il segnale di ripristino deve rispettare le seguenti condizioni.

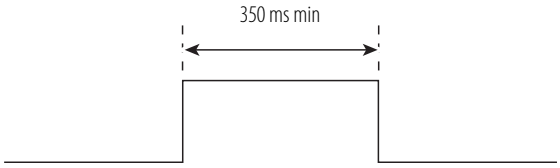
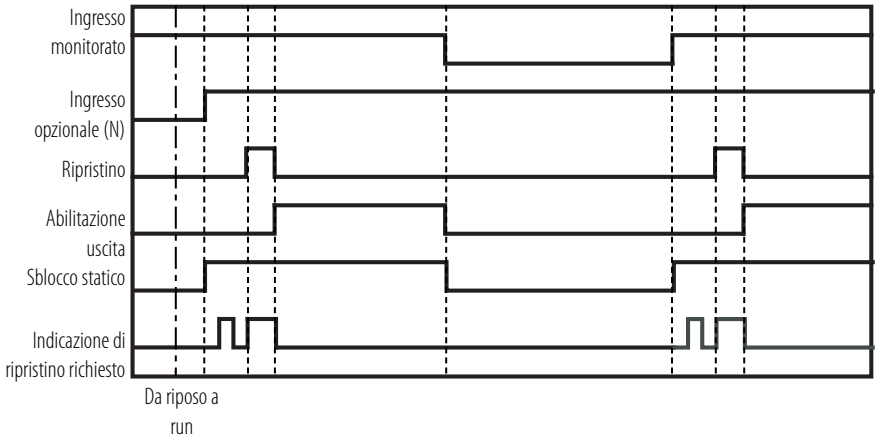
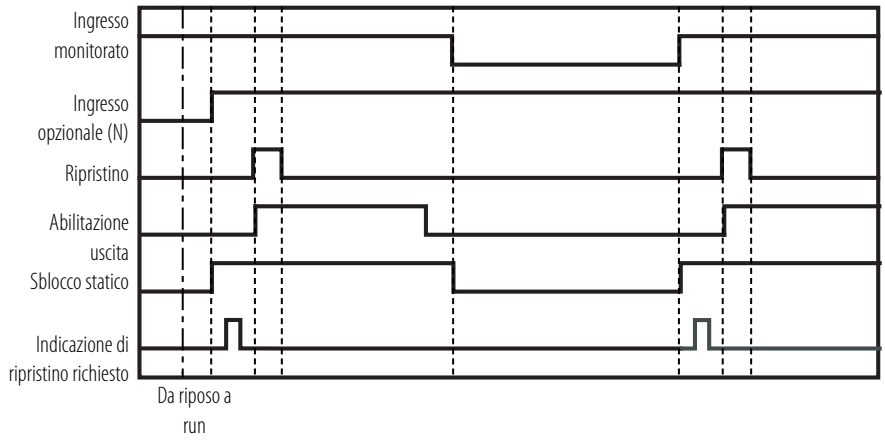


Diagramma dei tempi del blocco funzione Reset

Segnale di ripristino Low-High-Low

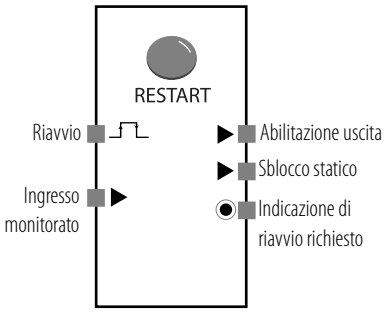


Fronte di salita del segnale di ripristino

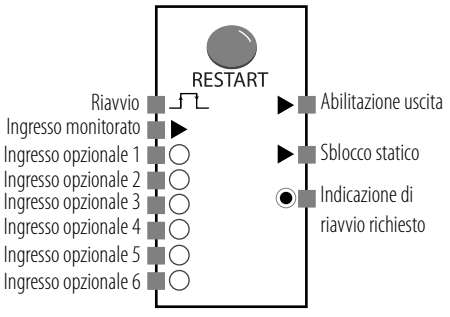


Blocco funzione Restart

Diagramma del blocco funzione Restart



Connessioni di default



N. massimo di ingressi per il blocco funzione Restart

È possibile portare il numero di ingressi da due a otto nella scheda I/O Settings della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet. Il numero di ingressi di default è due.

Il segnale di abilitazione uscita viene attivato se il segnale di riavvio viene ricevuto correttamente quando la condizione Ingresso monitorato del blocco funzione Restart è attivata. Questo blocco funzione può essere utilizzato per impedire che la macchina venga riavviata automaticamente all'accensione del controllore, quando la modalità operativa viene modificata o quando viene attivato un segnale proveniente da un dispositivo di ingresso di sicurezza. Da un punto di vista operativo, le funzioni Reset e Restart sono identiche.

Le uscite Sblocco statico e Indicazione di riavvio richiesto sono opzionali. Per abilitarle, selezionare la casella di controllo corrispondente nella scheda Out point della finestra di dialogo Function Block Properties.

Condizioni di attivazione delle uscite

Uscita	Condizione di attivazione
Abilitazione uscita	L'ingresso monitorato e tutti gli ingressi opzionali abilitati devono essere attivati ed è necessario che il segnale di riavvio venga ricevuto correttamente.
Sblocco statico	L'ingresso monitorato e tutti gli ingressi opzionali abilitati devono essere attivati.
Indicazione di riavvio richiesto	L'Indicazione di riavvio richiesto diventa un'uscita ad impulsi a 1 Hz se l'ingresso monitorato e tutti gli ingressi opzionali abilitati sono attivati e il segnale di abilitazione uscita è disattivato. L'Indicazione di riavvio richiesto viene attivata solo quando il segnale di riavvio è attivato.

Parametri del blocco funzione Restart

È possibile impostare il segnale di riavvio su Low-High-Low o su Rising Edge nella scheda Parameter della finestra di dialogo Function Block Properties. L'impostazione di default è Low-High-Low.

Con la configurazione Low-High-Low, il segnale di riavvio deve rispettare le seguenti condizioni.

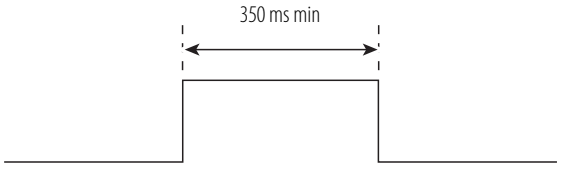
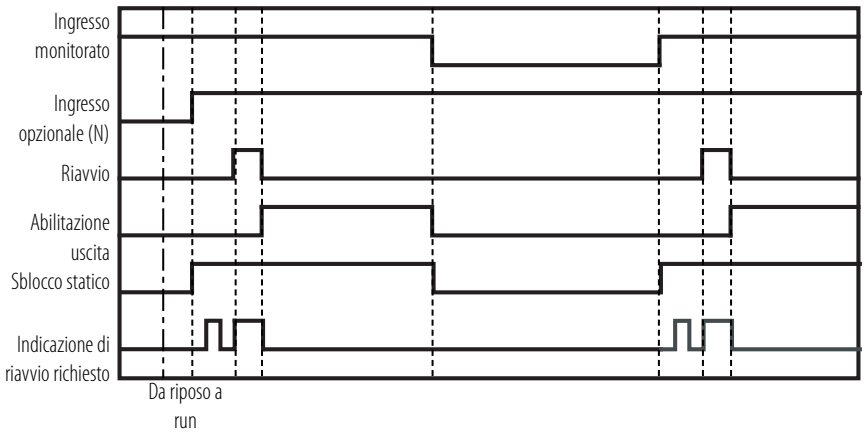
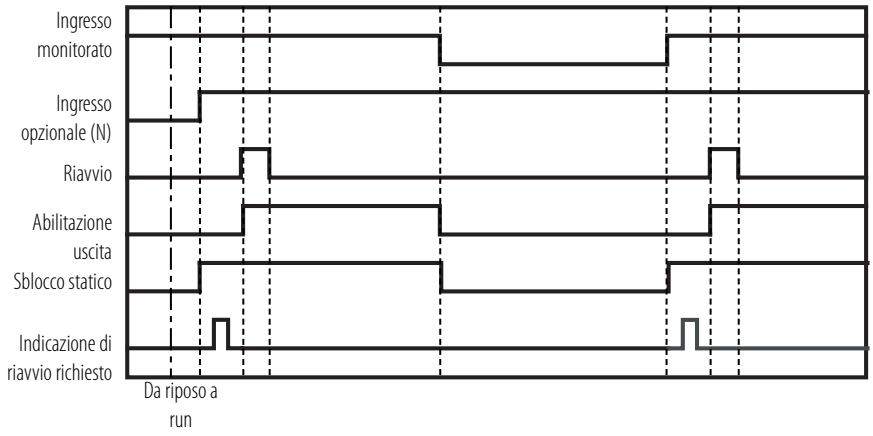


Diagramma dei tempi del blocco funzione Restart

Segnale di riavvio Low-High-Low

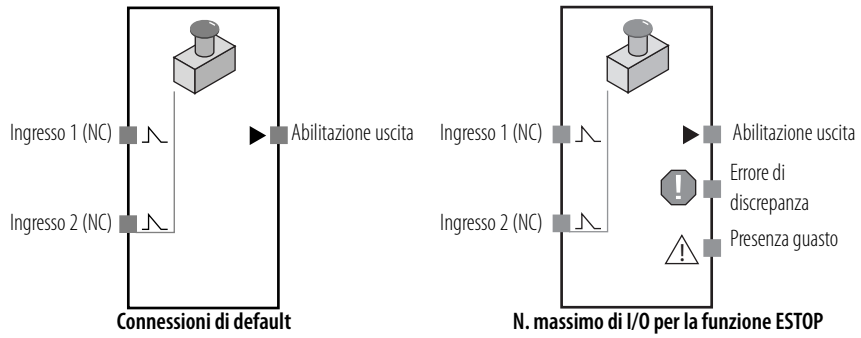


Fronte di salita del segnale di riavvio



Emergency Stop (ESTOP)

Diagramma del blocco funzione ESTOP



Connessioni di default **N. massimo di I/O per la funzione ESTOP**

La funzione Emergency Stop Pushbutton Monitoring consente di monitorare un pulsante di emergenza. Il segnale di abilitazione uscita viene attivato se gli ingressi del pulsante di emergenza monitorato sono attivi. Il segnale di abilitazione uscita viene disattivato se gli ingressi vengono disattivati o se viene rilevato un errore per il blocco funzione.

IMPORTANTE Per le applicazioni di arresto di emergenza è richiesta una funzione di ripristino manuale. Quando viene utilizzato il blocco funzione Emergency Stop Pushbutton, è necessario utilizzare anche il blocco funzione Reset.

L'uscita Errore di discrepanza può essere utilizzata per la programmazione del blocco funzione ESTOP. Per visualizzare questa uscita opzionale, selezionare la casella di controllo Discrepancy Error nella scheda Out point della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

Nella programmazione è possibile utilizzare anche l'uscita opzionale Fault Present. Per abilitare questa uscita opzionale, selezionare la casella di controllo Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Parametri del blocco funzione ESTOP

Impostare i seguenti parametri per il blocco funzione ESTOP.

Parametri del blocco funzione ESTOP

Parametro	Opzioni valide	Impostazione di default
Input Type	Single Channel, Dual Channel Equivalent Dual Channel Complementary	Doppio canale equivalente
Tempo di discrepanza	Da 0 a 30 s in incrementi di 10 ms.(1) Il tempo di discrepanza deve essere maggiore o uguale alla durata del ciclo del controllore.	30 ms

(1) Il controllo del tempo di discrepanza non viene eseguito se il tempo di discrepanza è impostato su 0.

Tabelle verità per il blocco funzione ESTOP

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per il blocco funzione ESTOP

Canale singolo		Doppio canale equivalente			Doppio canale complementare		
Ingresso 1 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NA)	Abilitazione uscita
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Gestione degli errori del blocco funzione ESTOP

Viene generato un errore di discrepanza quando uno degli ingressi risulta essere in uno stato non corretto per un periodo superiore al tempo di discrepanza. Ad esempio, nella modalità Canale duale equivalente, entrambi gli ingressi devono essere attivati (ON) entro il tempo di discrepanza, altrimenti si verifica un errore.

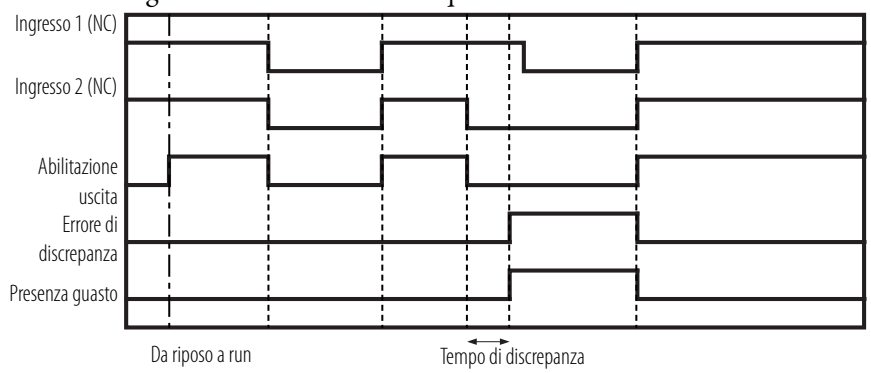
Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione ESTOP.

Rilevamento errori e ripristino per il blocco funzione ESTOP

Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita	Presenza guasto	Uscita errore	
Errore di discrepanza	OFF (Stato di sicurezza)	ON	Uscita errore di discrepanza: ON	Eliminare la causa dell'errore, quindi effettuare una delle operazioni seguenti: 1. attivare e disattivare gli ingressi 2. modificare la modalità operativa del controllore da riposo a run.

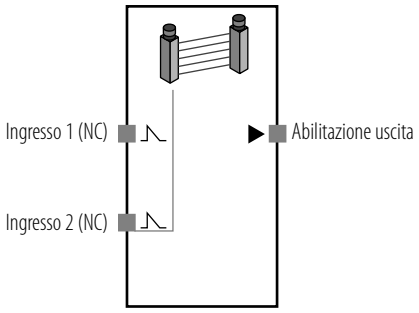
Diagramma dei tempi del blocco funzione ESTOP

Nel seguente diagramma vengono visualizzati i tempi di I/O con il blocco funzione configurato come canale duale equivalente.

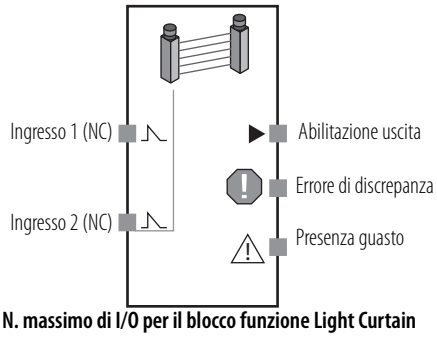


Blocco funzione LC (Light Curtain)

Diagramma del blocco funzione Light Curtain



Connessioni di default



N. massimo di I/O per il blocco funzione Light Curtain

Il blocco funzione Light Curtain monitoring monitora una barriera fotoelettrica di sicurezza di tipo 4. Il segnale di abilitazione uscita viene attivato quando gli ingressi della barriera fotoelettrica di sicurezza monitorata sono attivi. Il segnale di abilitazione uscita viene disattivato se gli ingressi vengono disattivati o se viene rilevato un errore per il blocco funzione.

È possibile utilizzare l'uscita Errore di discrepanza per la programmazione del blocco funzione LC. Per visualizzare questa uscita diagnostica opzionale, selezionare la casella di controllo Discrepancy Error nella scheda Out point della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

Nella programmazione è possibile utilizzare anche l'uscita opzionale Fault Present. Per abilitare questa uscita opzionale, selezionare la casella di controllo Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Parametri del blocco funzione Light Curtain

Impostare i seguenti parametri per il blocco funzione LC.

Parametri del blocco funzione LC

Parametro	Opzioni valide	Impostazione di default
Input Type	Dual Channel Equivalent Dual Channel Complementary	Doppio canale equivalente
Tempo di discrepanza	Da 0 a 30 s in incrementi di 10 ms.(1) Il tempo di discrepanza deve essere maggiore o uguale alla durata del ciclo del controllore.	30 ms

(1) Il controllo del tempo di discrepanza non viene eseguito se il tempo di discrepanza è impostato su 0.

Tabelle verità per il blocco funzione Light Curtain

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per il blocco funzione LC

Doppio canale equivalente			Doppio canale complementare		
Ingresso 1 (NC)	**Ingresso 2 (NC)**	**Abilitazione uscita**	**Ingresso 1 (NC)**	**Ingresso 2 (NC)**	**Abilitazione uscita**
0	0	0	0	0	0
0	1	0	0	1	0
1	0	0	1	0	1
1	1	1	1	1	0

Gestione degli errori del blocco funzione LC

Viene generato un errore di discrepanza quando uno degli ingressi risulta essere in uno stato non corretto per un periodo superiore al tempo di discrepanza. Ad esempio, nella modalità Canale duale equivalente, entrambi gli ingressi devono essere attivati (ON) entro il tempo di discrepanza, altrimenti si verifica un errore

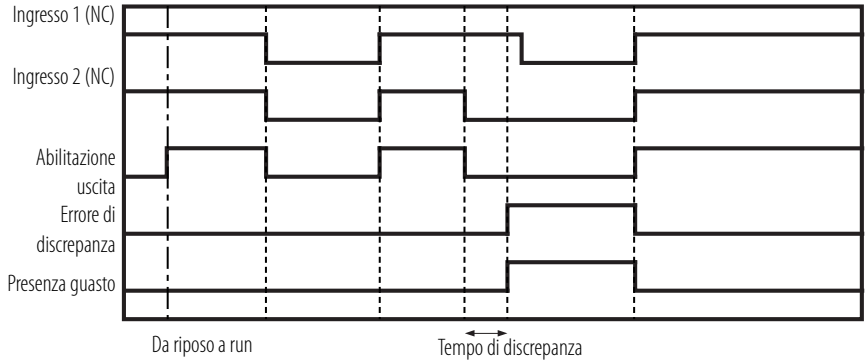
Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione LC.

Rilevamento errori e ripristino per il blocco funzione LC

Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita	**Presenza guasto**	**Uscita errore**	
Errore di discrepanza	OFF (Stato di sicurezza)	ON	Uscita errore di discrepanza: ON	Eliminare la causa dell'errore, quindi effettuare una delle operazioni seguenti: 1. Disattivare e riattivare gli ingressi. 2. modificare la modalità operativa del controllore da riposo a run.

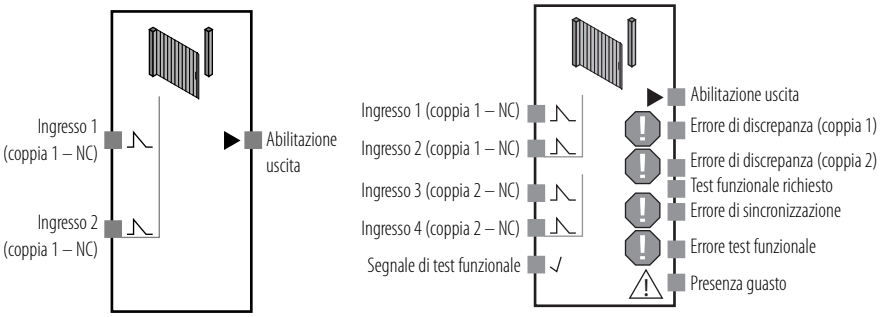
Diagramma dei tempi del blocco funzione Light Curtain

Nel seguente diagramma vengono visualizzati i tempi di I/O con il blocco funzione configurato come canale duale equivalente.



Blocco funzione Safety Gate Monitoring

Diagramma del blocco funzione Safety Gate Monitoring



Connessioni di default **N. massimo di I/O per la funzione Safety Gate**

La funzione Safety Gate Monitoring monitora lo stato di un interblocco di sicurezza utilizzando segnali di ingresso provenienti da un interruttore di interblocco di sicurezza o da un interruttore di finecorsa di sicurezza collegato all'interblocco. Il segnale di abilitazione uscita viene attivato se gli ingressi dell'interruttore monitorato sono attivi. Il segnale di abilitazione uscita viene disattivato se gli ingressi vengono disattivati o se viene rilevato un errore per il blocco funzione.

Uscite opzionali del blocco funzione Safety Gate Monitoring

Per la programmazione è possibile utilizzare anche le uscite opzionali. Per visualizzarle, selezionare la casella di controllo appropriata nella scheda Out point della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

- Errore di discrepanza coppia 1
- Errore di discrepanza coppia 2
- Segnale test funzionale richiesto
- Errore di sincronizzazione
- Errore test funzionale

Impostazione dell'uscita Presenza guasto del blocco funzione Safety Gate Monitoring

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Test funzionali del blocco funzione Safety Gate Monitoring

Per alcune applicazioni di interblocco di sicurezza, ad esempio le applicazioni di categoria 2, in caso di dispositivi di protezione è necessario verificare fisicamente che l'interblocco continui a funzionare correttamente.

Se il test funzionale è abilitato per il blocco funzione Safety Gate Monitoring, è possibile aggiungere come condizione per l'attivazione del segnale di abilitazione uscita un test dell'interblocco di sicurezza, in cui l'interblocco stesso deve essere fisicamente aperto e poi richiuso.

Se abilitato, il test dell'interblocco di sicurezza deve essere eseguito rispettando le seguenti condizioni.

- Avvio: il test dell'interblocco di sicurezza deve essere eseguito all'avvio del controllore, vale a dire quando la modalità operativa passa da riposo a RUN. Se il test viene completato correttamente, il segnale di abilitazione uscita viene attivato.
- Test funzionale richiesto dalla macchina: il test dell'interblocco di sicurezza deve essere eseguito dopo il rilevamento del controllore del segnale di test funzionale proveniente dalla macchina e l'attivazione e prima della riattivazione del segnale di test funzionale. Se il segnale di test funzionale viene attivato una seconda volta prima del completamento del test dell'interblocco di sicurezza, si verifica un errore del test funzionale, il segnale di abilitazione uscita viene disattivato e il segnale di errore del test funzionale viene attivato.
- Errore rilevato nel blocco funzione Safety Gate Monitoring: se si verifica un errore del test funzionale, un errore di discrepanza o un altro errore del blocco funzione, è necessario eseguire il test dell'interblocco di sicurezza dopo avere eliminato la causa dell'errore.

Il segnale di test funzionale richiesto proveniente dal blocco funzione Safety Gate Monitoring viene attivato quando è richiesto un test dell'interblocco di sicurezza e resta attivo finché il test non viene completato correttamente.

Parametri del blocco funzione Safety Gate Monitoring

Impostare i seguenti parametri per il blocco funzione Safety Gate Monitoring.

Parametri del blocco funzione Safety Gate Monitoring

Parametri	Opzioni	Default
Input Type	Single Channel Dual Channel Equivalent (1 pair) Dual Channel Complementary (1 pair) Two Dual Channel Equivalent (2 pairs) Two Dual Channel Complementary (2 pairs)	Doppio canale equivalente
Function Test	No Function Test/Function Test Required	Test funzionale non richiesto
Discrepancy Time Pair 1	0-30 s in incrementi di 10 ms. Se impostato su 0, non viene eseguito il controllo del tempo di discrepanza.	30 ms
Discrepancy Time Pair 2		
Synchronization Time	0-30 s in incrementi di 10 ms. Se impostato su 0, non viene eseguito il controllo del tempo di sincronizzazione.	300 ms

Tabelle verità per il blocco funzione Safety Gate Monitoring

Nelle tabelle verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per il blocco funzione Safety Gate Monitoring con canale singolo e canale duale (1 coppia)

Canale singolo		Doppio canale equivalente			Doppio canale complementare		
Ingresso 1 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NC)	Abilitazione uscita
0	0	0	0	0	0	0	0
1	1	0	1	0	0	1	0
--	--	1	0	0	1	0	1
--	--	1	1	1	1	1	0

Tabella verità per il blocco funzione Safety Gate Monitoring con canale duale (2 coppie)

Canale duale equivalente (2 coppie)					Canale duale complementare (2 coppie)				
Ingresso 1 (NC)	Ingresso 2 (NC)	Ingresso 3 (NC)	Ingresso 4 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NC)	Ingresso 3 (NC)	Ingresso 4 (NC)	Abilitazione uscita
0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0	1	0
0	0	1	0	0	0	0	1	0	0
0	0	1	1	0	0	0	1	1	0
0	1	0	0	0	0	1	0	0	0
0	1	0	1	0	0	1	0	1	0

Tabella verità per il blocco funzione Safety Gate Monitoring con canale duale (2 coppie)

Canale duale equivalente (2 coppie)					Canale duale complementare (2 coppie)				
Ingresso 1 (NC)	Ingresso 2 (NC)	Ingresso 3 (NC)	Ingresso 4 (NC)	Abilitazione uscita	Ingresso 1 (NC)	Ingresso 2 (NC)	Ingresso 3 (NC)	Ingresso 4 (NC)	Abilitazione uscita
0	1	1	0	0	0	1	1	0	0
0	1	1	1	0	0	1	1	1	0
1	0	0	0	0	1	0	0	0	0
1	0	0	1	0	1	0	0	1	0
1	0	1	0	0	1	0	1	0	1
1	0	1	1	0	1	0	1	1	0
1	1	0	0	0	1	1	0	0	0
1	1	0	1	0	1	1	0	1	0
1	1	1	0	0	1	1	1	0	0
1	1	1	1	1	1	1	1	1	0

Gestione degli errori del blocco funzione Safety Gate Monitoring

Viene generato un errore di discrepanza quando uno degli ingressi risulta essere in uno stato non corretto per un periodo superiore al tempo di discrepanza. Ad esempio, nella modalità Canale duale equivalente, entrambi gli ingressi devono essere attivati (ON) entro il tempo di discrepanza, altrimenti si verifica un errore.

Se vengono selezionate due coppie di ingressi e viene specificato un tempo di sincronizzazione, entrambi le coppie di ingressi devono trovarsi nello stesso stato entro il tempo di sincronizzazione, altrimenti si verifica un errore di sincronizzazione. Il tempo di discrepanza si applica ad entrambi gli ingressi della stessa coppia nello stesso stato entro il tempo specificato, mentre il tempo di sincronizzazione si applica ad entrambe le serie di coppie di ingressi nello stesso stato entro il tempo specificato.

Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione Safety Gate Monitoring.

Rilevamento errori e ripristino per il blocco funzione Safety Gate Monitoring

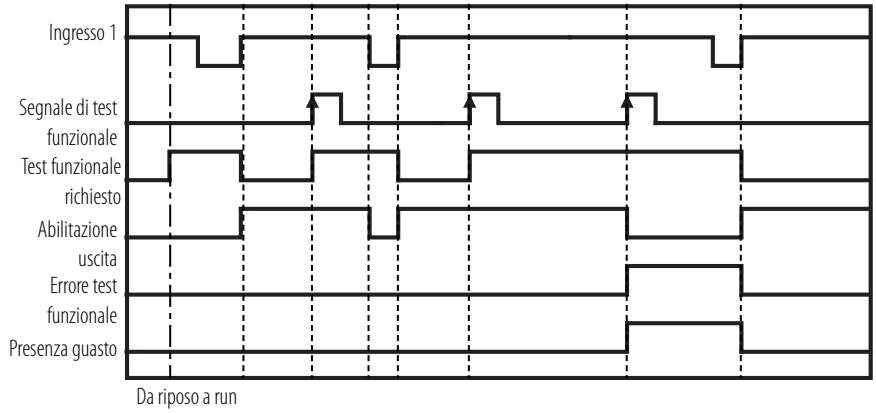
Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore	
	Abilitazione uscita	Presenza guasto	Uscita errore	Quando il test funzionale è disabilitato	Quando il test funzionale è abilitato
Errore di discrepanza per la coppia 1	OFF (Stato di sicurezza)	ON	Errore di discrepanza per la coppia 1: ON	Eliminare la causa dell'errore, quindi effettuare una delle operazioni seguenti: 1. Attivare e disattivare gli ingressi[2] 2. Modificare la modalità operativa del controllore da riposo a RUN.	Eliminare la causa dell'errore, quindi attivare e disattivare gli ingressi (vale a dire, eseguire il test dell'interblocco di sicurezza).
Errore di discrepanza per la coppia 2			Errore di discrepanza della coppia 2: ON		
Errore test funzionale[1]			Errore test funzionale: ON		
Errore di sincronizzazione			Errore test di sincronizzazione: ON		

(1) Il test dell'interblocco di sicurezza non è stato eseguito correttamente tra i segnali di test funzionale.

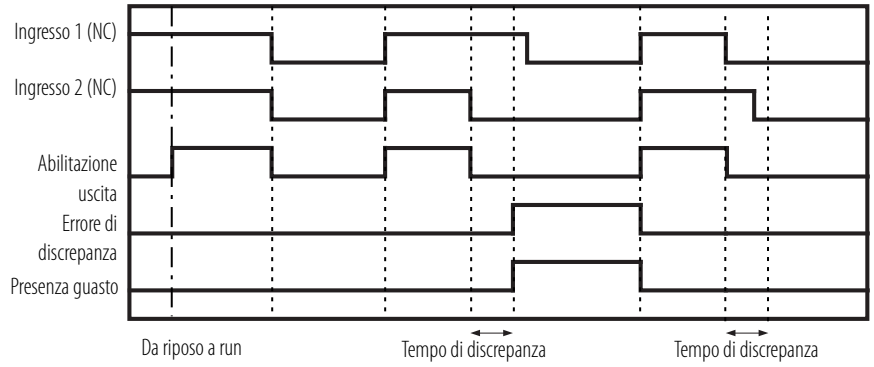
(2) Se si verifica un errore di discrepanza in una delle coppie con l'impostazione Canale duale equivalente (2 coppie) o Canale duale complementare (2 coppie), disattivare e riattivare le coppie di ingresso 1 e 2.

Diagramma dei tempi del blocco funzione Safety Gate Monitoring

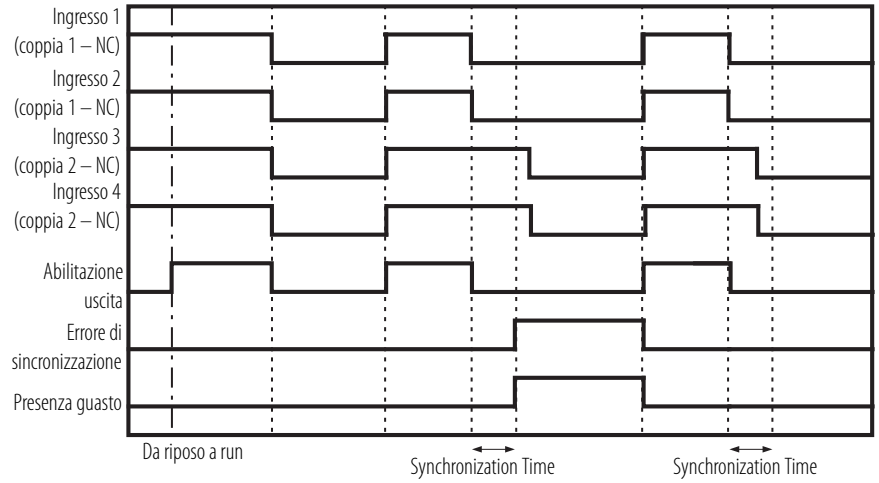
Canale singolo con test funzionale abilitato



Canale duale equivalente con test funzionale disabilitato

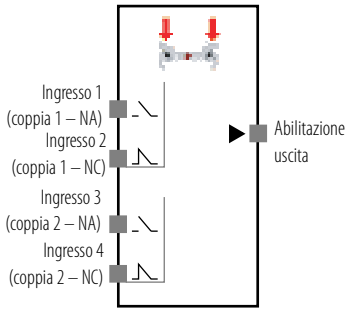


Canale duale equivalente (2 coppie) con test funzionale disabilitato

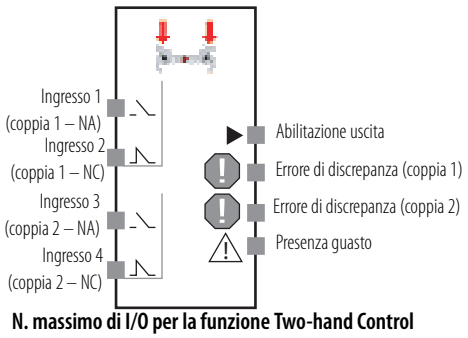


Blocco funzione Two-hand Control

Diagrammi del blocco funzione Two-hand Control



Connessioni di default



N. massimo di I/O per la funzione Two-hand Control

Il blocco funzione Two-hand Control consente di monitorare lo stato di un comando a due mani. Il blocco funzione Two-hand Control può essere utilizzato con un comando a due mani conforme ai requisiti dello standard EN 574 Tipo III C (Two-hand Control Devices, Functional Aspect – Principle for Design, Dispositivi di comando a due mani, Aspetti funzionali – Regole per la progettazione).

Il segnale di uscita viene attivato solo se entrambi gli ingressi del comando a due mani sono attivi e soddisfano i requisiti EN 574. Il segnale di abilitazione uscita viene disattivato se gli ingressi del comando a due mani non soddisfano i requisiti EN 574, se un ingresso è disattivato o se viene rilevato un errore nel blocco funzione.

Uscite opzionali del blocco funzione Two-hand Control

Per la programmazione è possibile utilizzare anche le uscite opzionali. Per visualizzarle, selezionare la casella di controllo appropriata nella scheda Out point della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

- Errore di discrepanza coppia 1
- Errore di discrepanza coppia 2

Impostazione dell'uscita Presenza guasto del blocco funzione Two-hand Control

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Parametri del blocco funzione Two-hand Control

Impostare i seguenti parametri per il blocco funzione Two-hand control.

Parametri del blocco funzione Two-hand Control

Parametro	Opzioni	Default
Discrepancy Time Input Pair 1	0-500 ms in incrementi di 10 ms.(1) I tempi di discrepanza devono essere maggiori o uguali alla durata del ciclo del controllore.	30 ms
Discrepancy Time Input Pair 2		

(1) Se il valore è impostato su 0, il controllo del tempo di discrepanza non viene eseguito.

Tabella verità per il blocco funzione Two-hand Control

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per il blocco funzione Two-hand Control

Ingresso 1 (coppia 1 – NA)	Ingresso 2 (coppia 1 – NC)	Ingresso 3 (coppia 2 – NA)	Ingresso 4 (coppia 2 – NC)	Abilitazione uscita
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	0
0	1	0	1	0
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	0

Gestione degli errori del blocco funzione Two-hand Control

Viene generato un errore di discrepanza quando uno degli ingressi risulta essere in uno stato non corretto per un periodo superiore al tempo di discrepanza. Ad esempio, nella modalità Canale duale equivalente, entrambi gli ingressi devono essere attivati (ON) entro il tempo di discrepanza, altrimenti si verifica un errore.

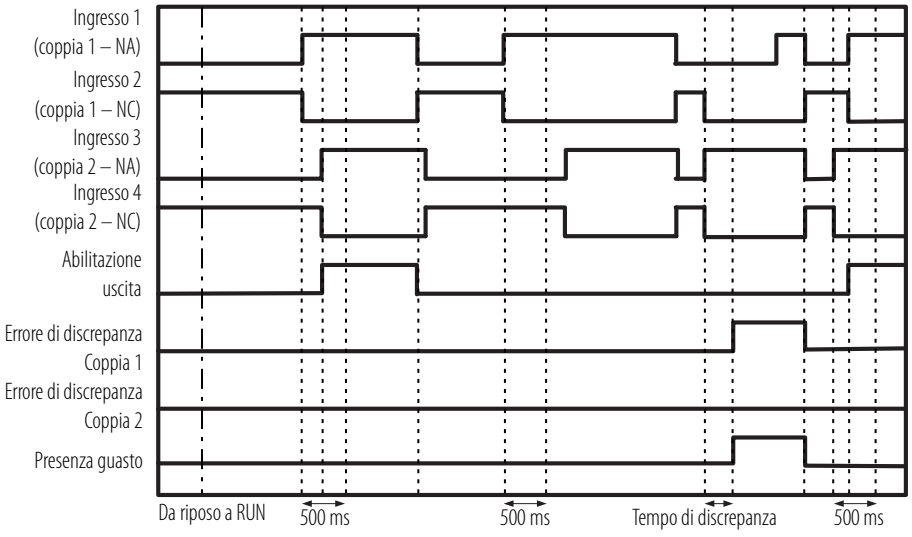
Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione Two-hand Control.

Rilevamento errori e ripristino per il blocco funzione Two-hand Control

Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita[1]	Presenza guasto	Uscita errore	
Errore di discrepanza per la coppia 1	OFF (Stato di sicurezza)	ON	Errore di discrepanza per la coppia 1: ON	Eliminare la causa dell'errore, quindi effettuare una delle operazioni seguenti: 1. Disattivare e riattivare entrambe le coppie di ingresso 1 e 2. 2. Modificare la modalità operativa del controllore da riposo a run.
Errore di discrepanza per la coppia 2			Errore di discrepanza della coppia 2: ON	

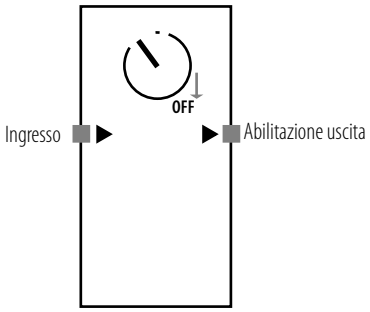
(1) Il segnale di abilitazione uscita non viene attivato se non viene soddisfatto il requisito del tempo di sincronizzazione (vale a dire, gli ingressi operativi per entrambe le mani devono essere completati entro 500 ms), ma tale condizione non viene considerata un errore.

Diagramma dei tempi del blocco funzione Two-hand Control



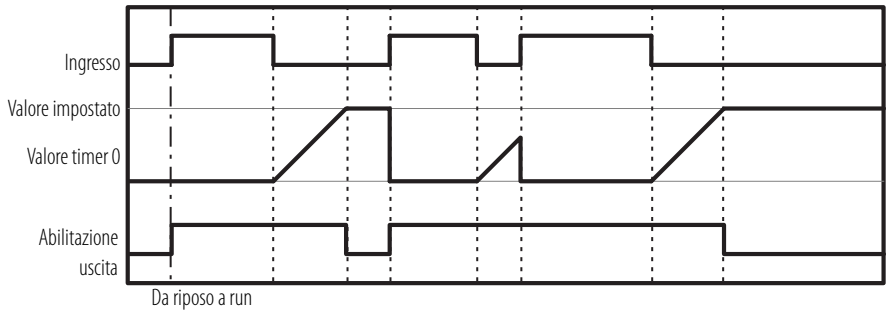
Blocco funzione OFF-delay Timer

Diagramma del blocco funzione OFF-delay Timer



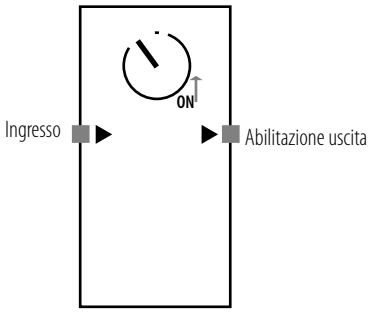
Il blocco funzione OFF-delay Timer esegue una funzione di temporizzazione con ritardo alla diseccitazione impostato in incrementi di 10 ms. L'intervallo di ritardo va da 0 ms a 300 secondi. L'impostazione di default è 0 ms.

Diagramma dei tempi del blocco funzione OFF-delay Timer



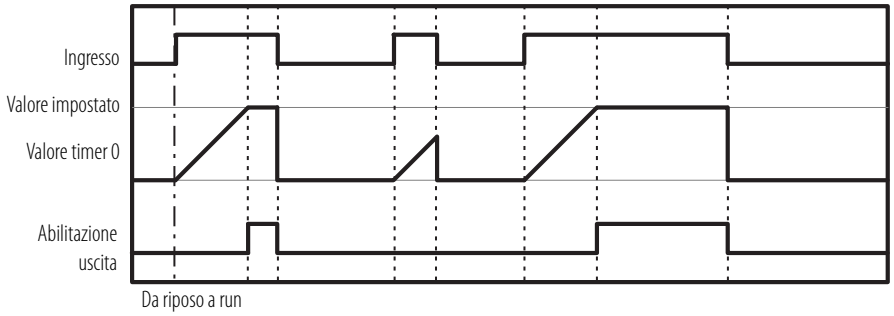
Blocco funzione ON-delay Timer

Diagramma del blocco funzione ON-delay Timer



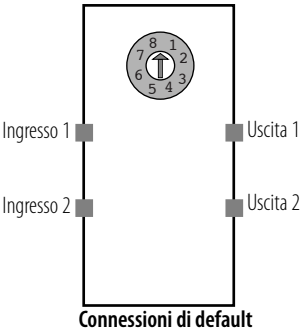
Il blocco funzione ON-delay Timer esegue una funzione di temporizzazione con ritardo all'eccitazione impostato in incrementi di 10 ms. L'intervallo di ritardo va da 0 ms a 300 secondi. L'impostazione di default è 0 ms.

Diagramma dei tempi del blocco funzione ON-delay Timer

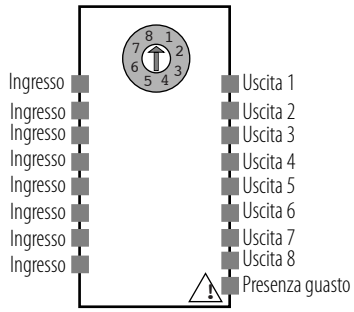


Blocco funzione User Mode Switch

Diagramma del blocco funzione User Mode Switch



Connessioni di default



N. massimo di ingressi per la funzione User Mode Switch

Il blocco funzione User Mode Switch viene utilizzato per monitorare un selettore della modalità operativa del dispositivo o del sistema utente. Il selettore della modalità operativa che può essere collegato a questo blocco funzione deve essere di tipo 1-di-N, vale a dire, uno dei contatti N è attivo (ON). Il blocco funzione supporta un massimo di otto ingressi con le relative otto uscite corrispondenti.

Uscite opzionali del blocco funzione User Mode Switch

È possibile aumentare il numero di I/O nella scheda In/Out Settings della finestra di dialogo Function Block Properties.

Impostare i seguenti parametri per le uscite opzionali.

Parametri delle uscite opzionali per il blocco funzione User Mode Switch

Parametro	Opzioni	Default
Number of Inputs	2…8	2
Number of Outputs	2…8	2

Impostazione dell'uscita Presenza guasto del blocco funzione User Mode Switch

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Use Fault Present nella scheda In/Out Setting della finestra di dialogo Function Block Properties.

Tabella verità per il blocco funzione User Mode Switch

Nella tabella verità, 0 equivale a disattivato e 1 ad attivato.

Tabella verità per il blocco funzione User Mode Switch

Ingressi								Uscite							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0
0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0
0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0
0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0
0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1

Gestione degli errori del blocco funzione User Mode Switch

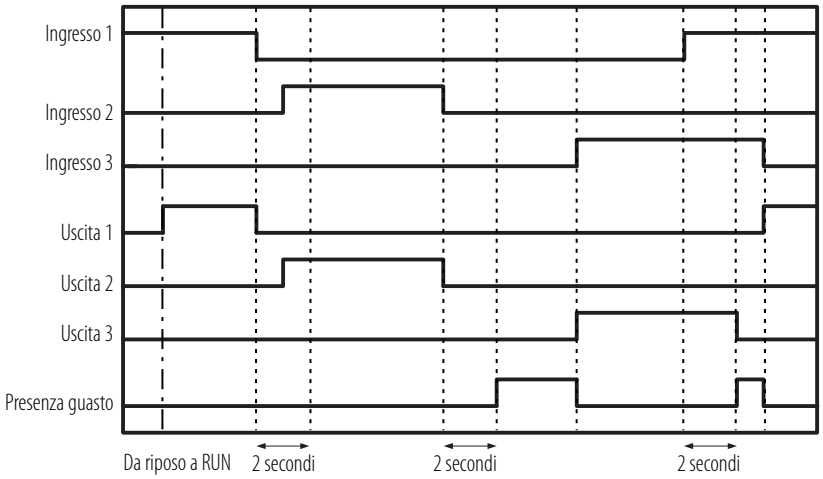
Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione User Mode Switch.

Rilevamento errori e ripristino per il blocco funzione User Mode Switch

Condizione di errore	Stato al verificarsi dell'errore		Per ripristinare la condizione di errore
	Uscita	Presenza guasto	
Sono stati attivati più ingressi per oltre 2 secondi.[1]	OFF (Stato di sicurezza)	ON	Correggere il sistema in modo che sia attivo un solo contatto.
Tutti gli ingressi sono stati disattivati per più di 2 secondi.			

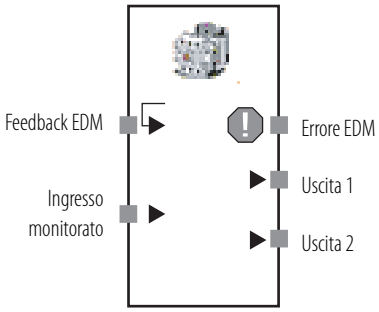
(1) Se sono attivi più ingressi nello stesso momento, l'uscita corrispondente al primo ingresso da attivare verrà attivata per 2 secondi.

Diagramma dei tempi del blocco funzione User Mode Switch

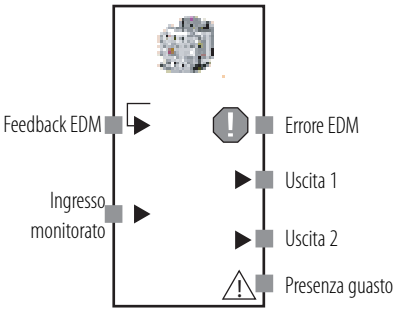


EDM (External Device Monitoring)

Diagramma del blocco funzione EDM



Connessioni di default



N. massimo di I/O per la funzione EDM

Il blocco funzione EDM (External Device Monitoring) valuta il segnale dell'ingresso monitorato e lo stato del segnale di feedback di un dispositivo esterno (feedback EDM), quindi attiva le uscite di sicurezza di un dispositivo esterno.

Se il segnale dell'ingresso monitorato viene attivato, anche i segnali dell'uscita 1 e dell'uscita 2 vengono attivati. In questo caso, lo stato del segnale di feedback deve cambiare entro il tempo specificato. Se il segnale dell'ingresso monitorato viene disattivato, anche i segnali dell'uscita 1 e dell'uscita 2 vengono disattivati. In questo caso, lo stato del segnale di feedback deve cambiare entro il tempo specificato.

Se lo stato del segnale di feedback non cambia entro il tempo specificato, si verifica un errore EDM, i segnali dell'uscita 1 e dell'uscita 2 vengono disattivati e il segnale di errore EDM viene attivato.

Uscite opzionali del blocco funzione EDM

Per la programmazione è possibile utilizzare anche le uscite opzionali. A tale fine, selezionare la casella di controllo appropriata nella scheda Out point della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

- Errore EDM
- Uscita 2

Impostazione dell'uscita Presenza guasto del blocco funzione EDM

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Use Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Parametro del blocco funzione EDM

Impostare il seguente parametro del blocco funzione EDM.

Parametro del blocco funzione EDM

Parametro	Opzioni	Default
EDM Feedback Maximum Time Delay (T_{EDM})	Da 100 a 1000 ms in incrementi di 10 ms	300 ms

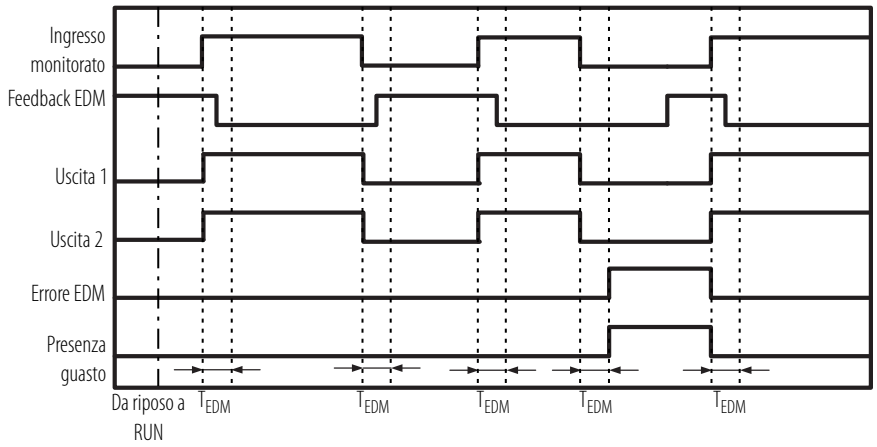
Gestione degli errori del blocco funzione EDM

Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione EDM.

Rilevamento errori e ripristino per il blocco funzione EDM

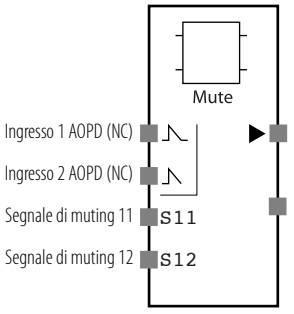
Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita	Presenza guasto	Uscita errore	
Errore di feedback EDM	OFF (Stato di sicurezza)	ON	Uscita errore EDM: ON	Eliminare la causa dell'errore e attivare l'ingresso di sicurezza.

Diagramma dei tempi del blocco funzione EDM

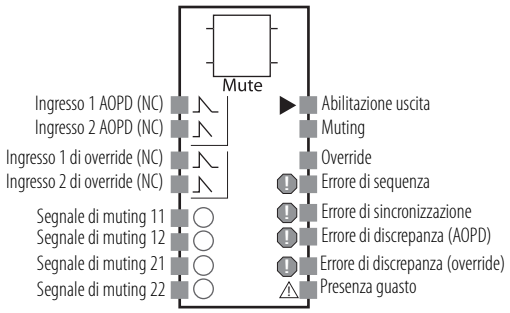


Muting

Diagrammi del blocco funzione Muting



Connessioni di default



N. massimo di I/O per la funzione Muting

Il blocco funzione Muting disabilita temporaneamente il segnale di interruzione del fascio luminoso (ingresso AOPD, dispositivo di protezione optoelettrico attivo) in una barriera fotoelettrica mentre il sensore di muting è in fase di attivazione. Quando la funzione di muting è attiva, il funzionamento della macchina non viene interrotto, pertanto è possibile rimuovere un oggetto dalla zona di rilevamento della barriera fotoelettrica. Inoltre, il blocco funzione Muting dispone di una funzione di annullamento (override) che può disabilitare il segnale di interruzione del fascio luminoso della barriera fotoelettrica consentendo il funzionamento della macchina mentre la luce della barriera fotoelettrica è bloccata. Ad esempio, in caso di un oggetto bloccato nella zona di rilevamento della barriera fotoelettrica, è possibile controllare la macchina in modo da consentirne la rimozione.

Parametri del blocco funzione Muting

Impostare i seguenti parametri per il blocco funzione Muting.

Parametri del blocco funzione Muting

Parametro	Impostazioni/Intervallo	Default
Muting Mode	• Parallel muting with 2 sensors Questo modello è ideale per le applicazioni all'entrata di un trasportatore. Utilizzarlo quando sono configurati due sensori fotoelettrici a riflessione come sensori di muting con zone di rilevamento incrociate. • Sequential muting (forward direction) Questo modello è ideale per le applicazioni all'entrata di un trasportatore. Utilizzarlo quando sono configurati quattro sensori fotoelettrici a sbarramento come sensori di muting. • Sequential muting (both directions) Questo modello è ideale per le applicazioni all'entrata o all'uscita di un trasportatore. Utilizzarlo quando sono configurati quattro sensori fotoelettrici a sbarramento come sensori di muting. • Position detection Questo modello è ideale per le applicazioni in cui il muting è controllato da un ingresso interruttore. Utilizzarlo per disabilitare temporaneamente il segnale di interruzione del fascio luminoso della barriera fotoelettrica quando un operatore posiziona un oggetto nell'apertura della macchina e lo stato della macchina è tale da non costituire alcun pericolo per l'operatore (i pericoli risiedono in una zona differente della macchina). In tutte le descrizioni delle impostazioni, i sensori di muting sono attivati quando viene eseguito il rilevamento e disattivati in caso contrario.	Parallel muting with 2 sensors
Synchronization Time[1]	Da 30 ms a 3 secondi in incrementi di 10 ms. Il valore impostato per il timer deve essere superiore alla durata del ciclo del controllore.	3 secondi
Input Type of AOPD	• Dual Channel Equivalent (NC/NC) • Dual Channel Complementary (NC/NO)	Doppio canale equivalente
Discrepancy Time (AOPD)	Da 10 a 500 ms in incrementi di 10 ms[2] Il valore impostato per il timer deve essere superiore alla durata del ciclo del controllore.	30 ms
Input Type of Override Signal	• Canale singolo • Dual Channel Equivalent (NO/NO) • Dual Channel Complementary (NC/NO) • Non utilizzato	Not used
Discrepancy Time (Override)	Da 10 a 500 ms in incrementi di 10 ms[2] Il valore impostato per il timer deve essere superiore alla durata del ciclo del controllore.	30 ms
Max Muting Time	Da 500 ms a 127,5 secondi in incrementi di 500 ms Da 0 a 500 ms in incrementi di 10 ms	60 secondi
Max Override Time	Da 500 ms a 127,5 secondi in incrementi di 500 ms	60 secondi

(1) Tra il segnale di muting 11 e il segnale di muting 12 o tra il segnale di muting 21 e il segnale di muting 22.

(2) Se il valore è impostato su 0, il controllo del tempo di discrepanza non viene eseguito.

Uscite opzionali del blocco funzione Muting

Per la programmazione è possibile utilizzare anche le uscite opzionali. A tale fine, selezionare la casella di controllo appropriata nella scheda In/Out Setting della finestra di dialogo Function Block Properties nello strumento Logic Editor del software RSNetWorx for DeviceNet.

- Override
- Errore di sincronizzazione
- Errore di sequenza
- Errore di discrepanza (AOPD)
- Errore di discrepanza (override)

Impostazione dell'uscita Presenza guasto del blocco funzione Muting

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Use Fault Present nella scheda In/Out Setting della finestra di dialogo Function Block Properties.

Gestione degli errori del blocco funzione Muting

Utilizzare la tabella seguente per individuare e ripristinare le condizioni di errore nel blocco funzione Muting.

Rilevamento errori e ripristino per il blocco funzione Muting

Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita	Presenza guasto	Uscita errore[3]	
Errore di sincronizzazione (tra il segnale di muting 11 e il segnale di muting 12 o tra il segnale di muting 21 e il segnale di muting 22)[1]	ON[2]	OFF[2]	Errore di sincronizzazione: ON	Applicare nuovamente il muting oppure modificare la modalità operativa del controllore impostandola su riposo, quindi su RUN.
Errore di sequenza			Errore di sequenza: ON	
Errore di discrepanza (AOPD)	OFF (Stato di sicurezza)	ON	Errore di discrepanza (AOPD): ON	Eseguire il ripristino quando entrambi i segnali di ingresso della barriera fotoelettrica passano dallo stato inattivo ad attivo oppure se la modalità operativa del controllore viene modificata e impostata su riposo, quindi su RUN.
Errore di discrepanza (override)			Errore di discrepanza (override): ON	Eseguire il ripristino quando entrambi i segnali di ingresso di override passano dallo stato inattivo ad attivo oppure se la modalità operativa del controllore viene modificata e impostata su riposo, quindi su RUN.

(1) Questo errore viene rilevato solo nella modalità di muting sequenziale (bidirezionale).

(2) Se la barriera fotoelettrica passa da questo stato di errore allo stato di inattività (assenza di luce), il segnale di abilitazione uscita verrà disattivato e il segnale di Presenza guasto verrà attivato. Se la barriera fotoelettrica diventa attiva (luce incidente) oppure viene eseguita la funzione di override, il segnale di abilitazione uscita verrà attivato e il segnale di Presenza guasto verrà disattivato.

(3) Se si verificano più errori, essi verranno segnalati per tutte le uscite di errore interessate.

Dettagli sulla funzione Muting

Nelle sezioni seguenti vengono descritte le condizioni di ripristino, di avvio e di arresto del blocco funzione Muting.

Condizioni di ripristino

L'uscita di sicurezza (Abilitazione uscita) viene attivata quando vengono rispettate tutte le condizioni seguenti.

- Il segnale della barriera fotoelettrica è attivo (luce incidente).
- Non si è verificato un errore di discrepanza.

Condizioni di avvio

Se vengono rispettate le seguenti condizioni per i sensori di muting mentre il segnale di abilitazione uscita è attivato, il muting viene applicato e il segnale di muting viene attivato:

- i sensori di muting sono tutti disattivati
- mentre i sensori di muting sono disattivati, due sensori di muting rilevano un oggetto nella sequenza corretta
- mentre i sensori di muting sono disattivati, i tempi di sincronizzazione dei due sensori di muting rientrano nell'intervallo normale (esclusa l'impostazione di rilevamento posizione).

Se si verifica un errore, viene generata un'uscita di allarme. Il segnale di errore di sequenza viene attivato in caso di sequenza non valida. Il segnale di errore di sincronizzazione viene attivato se un oggetto non viene rilevato entro il tempo di sincronizzazione. L'uscita di sicurezza (Abilitazione uscita) viene disattivata se il segnale della barriera fotoelettrica non è attivo (assenza di luce) prima che il controllore passi nello stato di muting.

Condizioni di arresto

Se vengono rispettate le seguenti condizioni mentre la funzione di muting è attivata, il muting viene arrestato e il segnale di muting disattivato:

- due o più sensori sono disattivati
- il tempo massimo di muting è trascorso
- si è verificato un errore di discrepanza.

L'uscita di sicurezza viene disattivata (Abilitazione uscita) se il muting viene arrestato e la barriera fotoelettrica bloccata.

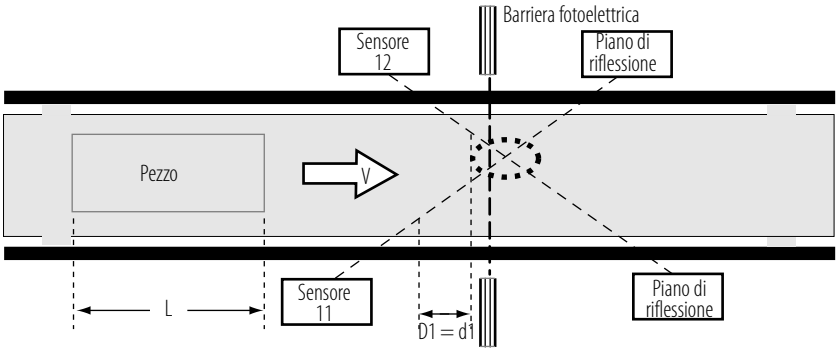
IMPORTANTE

Quando la modalità operativa del controllore SmartGuard viene modificata da riposo a RUN, i dati di ingresso degli slave non sono disponibili finché non viene ristabilita la comunicazione. Se i dati di ingresso degli slave vengono utilizzati per l'ingresso del dispositivo di protezione optoelettrico attivo, le uscite Presenza guasto e Errore di sequenza vengono attivate non appena la modalità operativa passa a RUN. Quando l'ingresso del dispositivo di protezione optoelettrico attivo viene attivato, l'uscita Presenza guasto viene disattivata. Quando la condizione di avvio del muting viene rispettata, l'uscita Errore di sequenza viene disattivata.

Esempio: muting in parallelo con 2 sensori

In questo esempio due sensori fotoelettrici a riflessione sono configurati come sensori di muting con zone di rilevamento incrociate. L'intersezione dei due sensori deve trovarsi dietro la barriera fotoelettrica. Utilizzare questa configurazione quando la lunghezza del pezzo (L) non è fissa o non è sufficiente per attivare i sensori di muting sequenziale.

Configurazione dell'applicazione



Il sensore 12 è collegato al segnale di muting 12. Il sensore 11 è collegato al segnale di muting 11.

Sequenza di muting

Di seguito viene descritta la sequenza di muting per il presente esempio.

1. La luce non viene interrotta tra i sensori 11 e 12 e la barriera fotoelettrica, pertanto il segnale di abilitazione uscita è attivato.
2. Con l'avanzamento del pezzo verso destra e l'attivazione dei sensori 11 e 12 in sequenza, il muting viene abilitato.
3. Man mano che il pezzo continua ad avanzare, il segnale di abilitazione uscita viene mantenuto attivo anche se la barriera fotoelettrica viene bloccata.
4. Man mano che il pezzo continua ad avanzare, la luce proveniente dal sensore 11 non viene più interrotta dal pezzo, lo stato di muting viene azzerato e il segnale di muting disattivato.

Impostazioni delle distanze

Quando vengono configurate applicazioni di questo tipo, le impostazioni delle distanze devono impedire che il passaggio di una persona abiliti la funzione di muting e la barriera fotoelettrica e i sensori di muting devono essere configurati in modo tale che il pezzo passi da tutti i sensori di muting prima che il pezzo successivo arrivi nei sensori di muting.

Per calcolare le distanze appropriate da impostare per il presente esempio, utilizzare le formule seguenti, in cui:

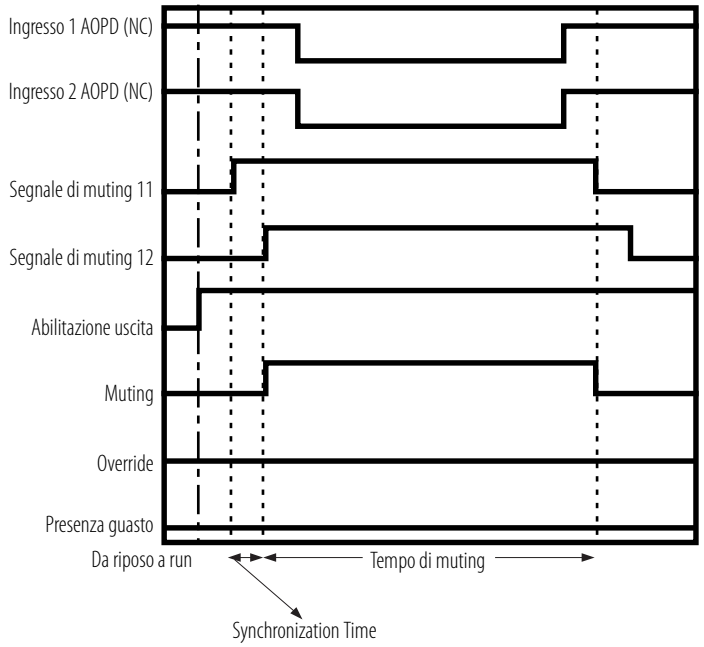
D1 = distanza minima richiesta per le prestazioni dei sensori di muting
d1 = distanza massima richiesta per le prestazioni dei sensori di muting
L = lunghezza del pezzo
V = velocità di transito del pezzo
T1min = durata del ciclo del controllore
T1max= impostazione del tempo di sincronizzazione (l'impostazione di default è 3 secondi)

Formula 1: D1 < L
Formula 2: V x T1min < d1 < V x T1max

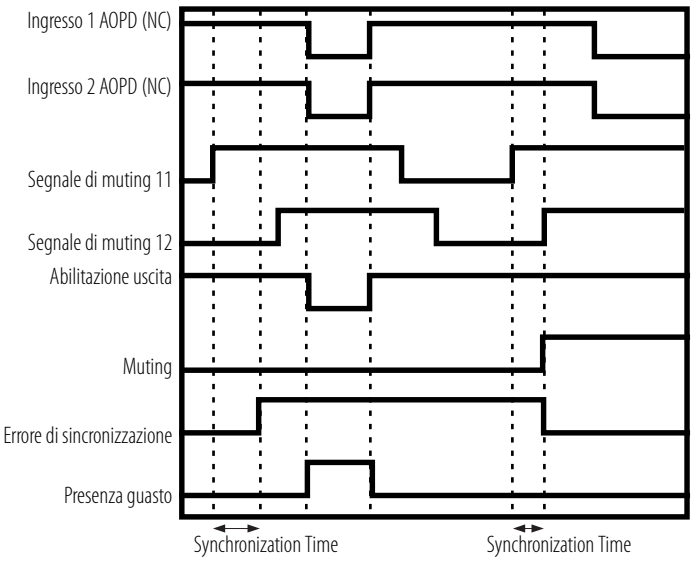
Per il funzionamento efficiente della funzione di muting, entrambe le formule devono essere soddisfatte.

Diagramma dei tempi del muting sequenziale (in avanti)

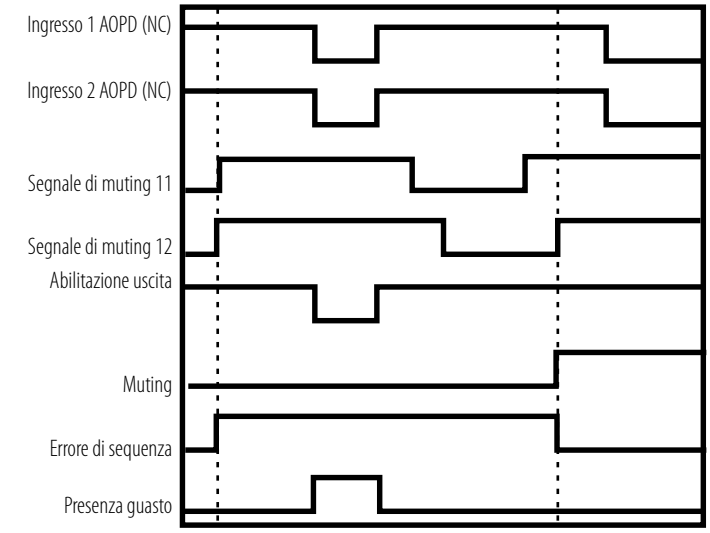
Funzionamento normale



Errore di sincronizzazione



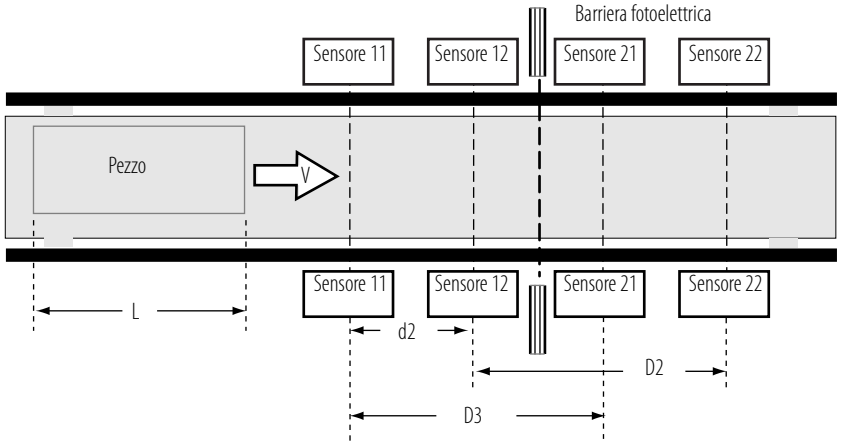
Errore di sequenza



Esempio: muting sequenziale con 4 sensori (in avanti)

In questo esempio quattro sensori fotoelettrici a sbarramento sono configurati come sensori di muting con zone di rilevamento incrociate. Utilizzare questa configurazione quando la lunghezza del pezzo trasportato è fissa e sufficiente per attivare i sensori di muting montati in sequenza.

Configurazione dell'applicazione



Il sensore 11 è collegato al segnale di muting 11. Il sensore 12 è collegato al segnale di muting 12. Il sensore 21 è collegato al segnale di muting 21. Il sensore 22 è collegato al segnale di muting 22.

Sequenza di muting

Di seguito viene descritta la sequenza di muting per questo esempio.

1. La luce non viene interrotta tra i sensori 11, 12, 21 e 22 e la barriera fotoelettrica, pertanto il segnale di abilitazione uscita è attivato.

2. Con l'avanzamento del pezzo verso destra e l'attivazione dei sensori 11 e 12 in sequenza, il muting viene abilitato e il segnale di muting viene attivato.

3. Man mano che il pezzo continua ad avanzare, il segnale di abilitazione uscita viene mantenuto attivo anche se la barriera fotoelettrica viene bloccata.

4. Man mano che il pezzo continua ad avanzare, la luce proveniente dal sensore 21 non viene più interrotta dal pezzo, lo stato di muting viene azzerato e il segnale di muting disattivato.

Impostazioni delle distanze

Quando vengono configurate applicazioni di questo tipo, le impostazioni delle distanze devono impedire che il passaggio di una persona abiliti la funzione di muting e la barriera fotoelettrica e i sensori di muting devono essere configurati in modo tale che il pezzo passi da tutti i sensori di muting prima che il pezzo successivo arrivi nei sensori di muting.

Per calcolare le distanze appropriate da impostare per il presente esempio, utilizzare le formule seguenti, in cui:

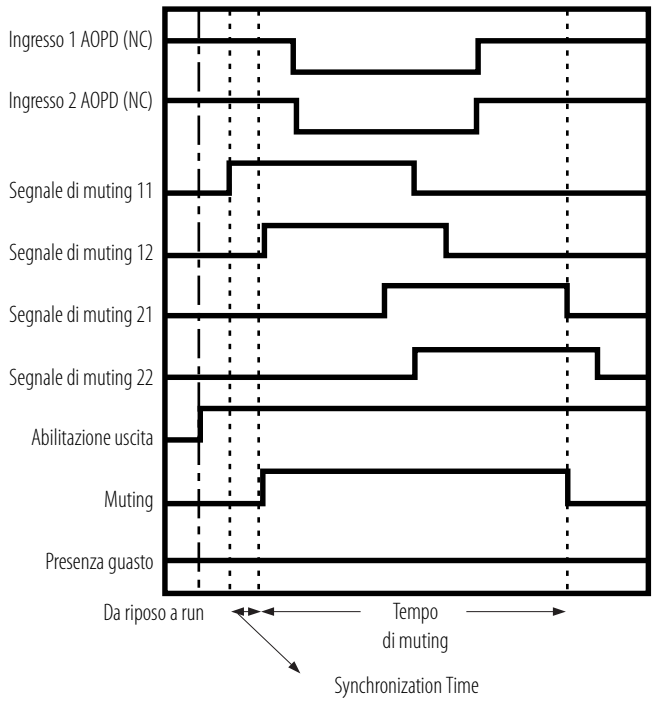
D2 e D3 = distanza minima richiesta per le prestazioni dei sensori di muting
d2 = distanza massima richiesta per le prestazioni dei sensori di muting
L = lunghezza del pezzo
V = velocità di transito del pezzo
T1min = durata del ciclo del controllore
T1max= impostazione del tempo di sincronizzazione (l'impostazione di default è 3 secondi)

Formula 3: $D2 < L$
Formula 4: $D3 < L$
Formula 5: $V \times T1min < d2 < V \times T1max$

Per il funzionamento efficiente della funzione di muting, le formule 3, 4 e 5 devono essere soddisfatte.

Diagramma dei tempi del muting sequenziale (in avanti)

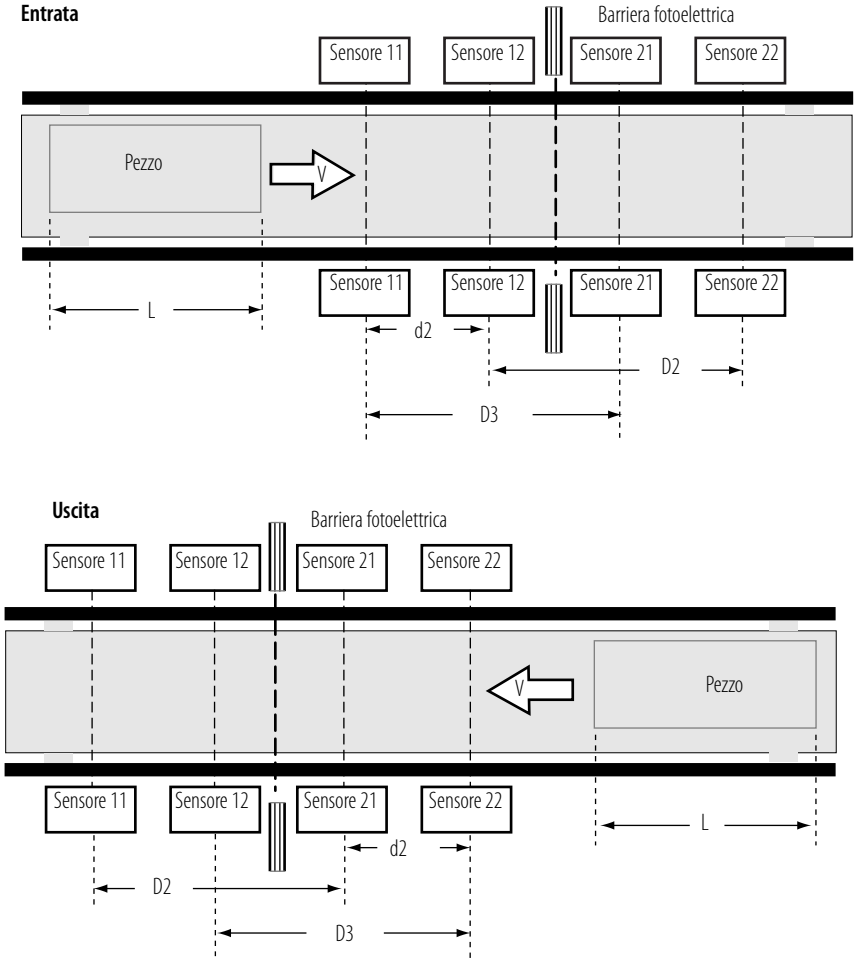
Funzionamento normale



Esempio: muting sequenziale con 4 sensori (bidirezionale)

In questo esempio quattro sensori fotoelettrici a sbarramento sono configurati come sensori di muting con zone di rilevamento incrociate.

Configurazione dell'applicazione



Il sensore 11 è collegato al segnale di muting 11. Il sensore 12 è collegato al segnale di muting 12. Il sensore 21 è collegato al segnale di muting 21. Il sensore 22 è collegato al segnale di muting 22.

Sequenza di muting

Di seguito viene descritta la sequenza di muting per il presente esempio.

1. La luce non viene interrotta tra i sensori 11, 12, 21 e 22 e la barriera fotoelettrica, pertanto il segnale di abilitazione uscita è attivato.

2. Per l'entrata, con l'avanzamento del pezzo verso destra e l'attivazione dei sensori 11 e 12 in sequenza (i sensori 21 e 22 si attivano man mano che il pezzo esce), il muting viene abilitato e il segnale di muting viene attivato.

3. Man mano che il pezzo continua ad avanzare, il segnale di abilitazione uscita viene mantenuto attivo anche se la barriera fotoelettrica viene bloccata.

4. Man mano che il pezzo continua ad avanzare, non viene più rilevato dal sensore 21 nell'entrata (sensore 12 durante l'uscita del pezzo), lo stato di muting viene azzerato e il segnale di muting disattivato.

Impostazioni delle distanze

Quando vengono configurate applicazioni di questo tipo, le impostazioni delle distanze devono impedire che il passaggio di una persona abiliti la funzione di muting e la barriera fotoelettrica e i sensori di muting devono essere configurati in modo tale che il pezzo passi da tutti i sensori di muting prima che il pezzo successivo arrivi nei sensori di muting.

Per calcolare le distanze appropriate da impostare per il presente esempio, utilizzare le formule seguenti, in cui:

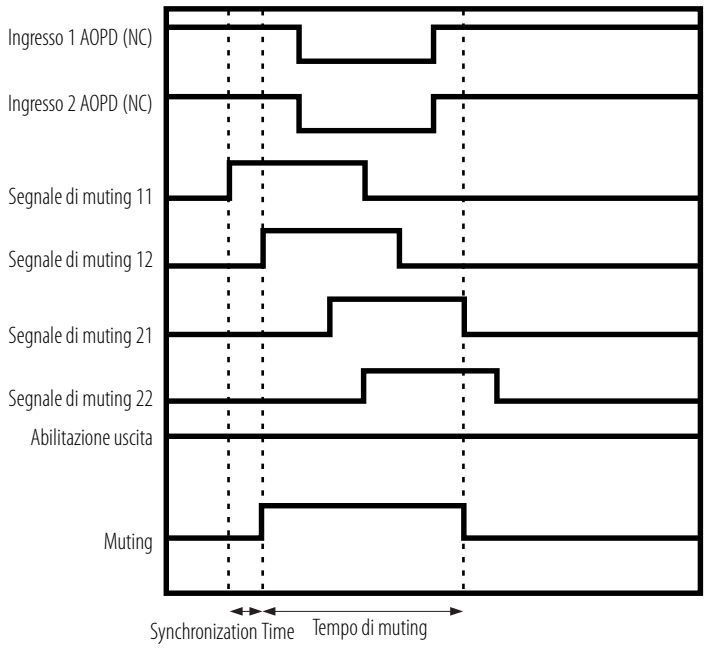
D2 e D3 = distanza minima richiesta per le prestazioni dei sensori di muting
d2 = distanza massima richiesta per le prestazioni dei sensori di muting
L = lunghezza del pezzo
V = velocità di transito del pezzo
T1min = durata del ciclo del controllore
T1max= impostazione del tempo di sincronizzazione (l'impostazione di default è 3 secondi)

Formula 3: D2 < L
Formula 4: D3 < L
Formula 5: V x T1min < d2 < V x T1max

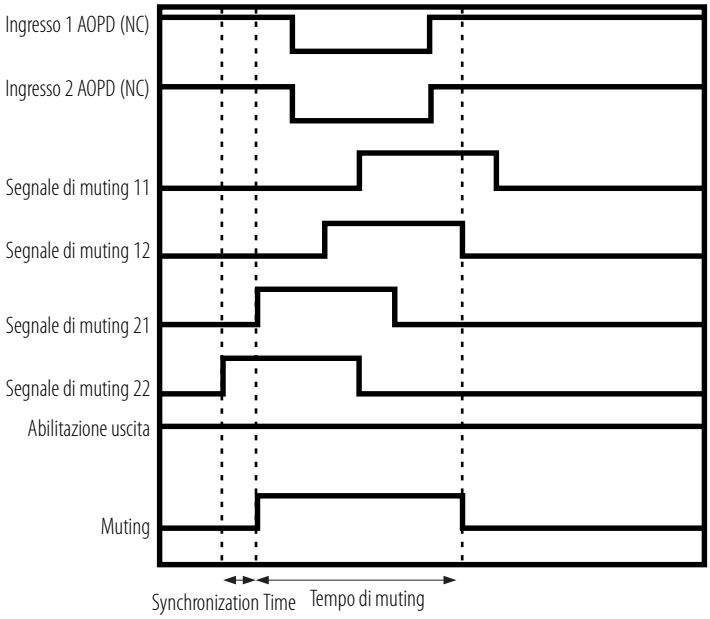
Per il funzionamento efficiente della funzione di muting, le formule 3, 4 e 5 devono essere soddisfatte.

Diagrammi dei tempi del muting sequenziale (bidirezionale)

Diagramma dei tempi dell'entrata



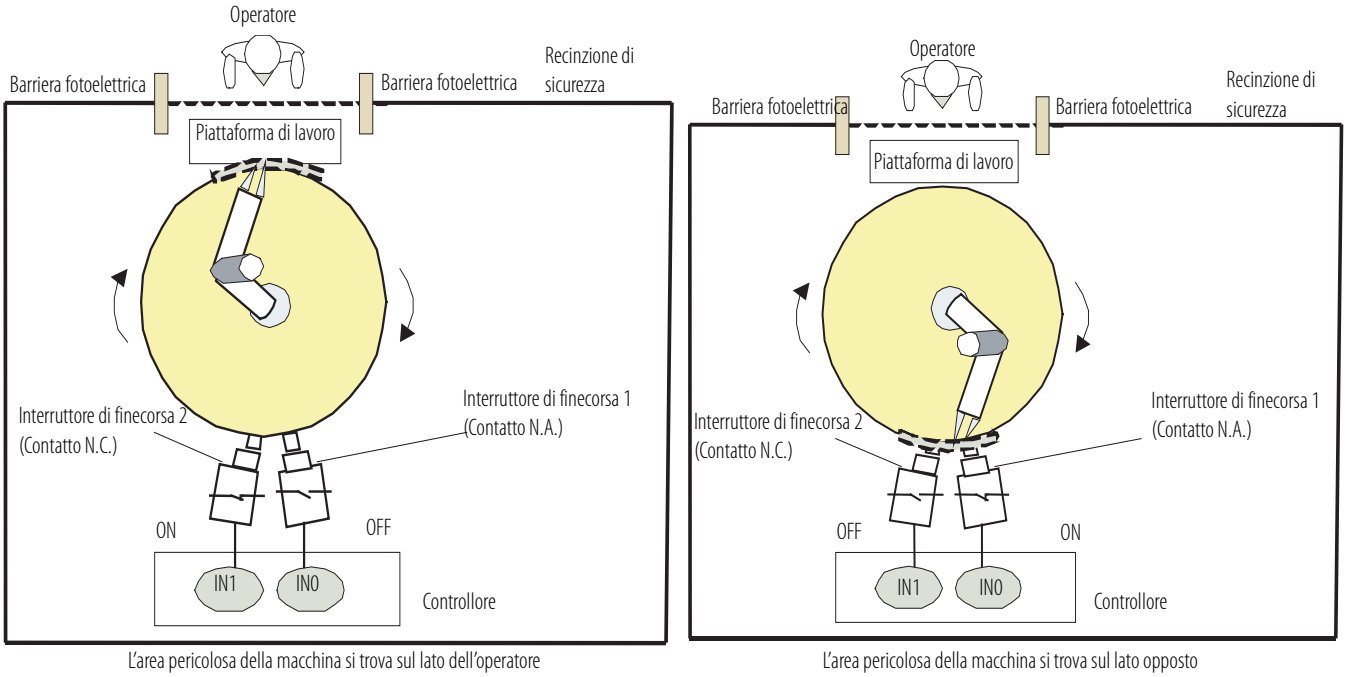
Modello 2 di ingresso con differenza di tempi: diagramma dei tempi dell'uscita



Esempio: rilevamento posizione

Nella seguente applicazione di esempio, il pezzo è montato su una tavola rotante circondata da una recinzione di protezione. L'operatore può disabilitare il segnale di interruzione del fascio luminoso della funzione di sicurezza della barriera fotoelettrica per posizionare un pezzo sulla tavola rotante quando l'area pericolosa della macchina si trova sul lato opposto all'operatore.

Configurazione dell'applicazione

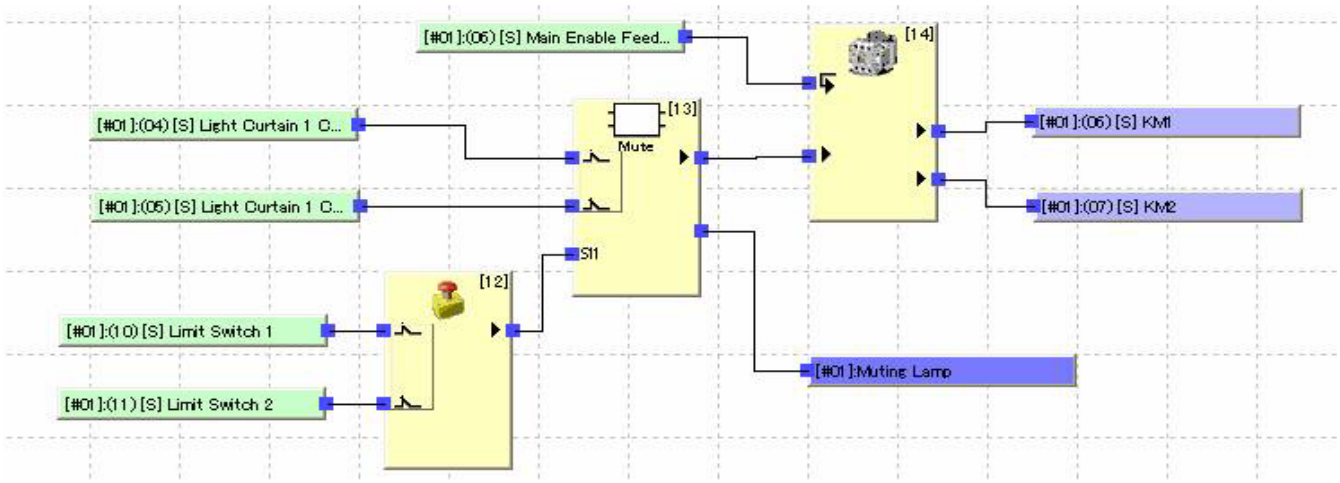


Configurare l'ingresso locale del controllore come canale duale complementare.

Esempio di programma

Gli interruttori di finecorsa 1 e 2 sono collegati al segnale di muting 11 del blocco funzione Muting che utilizza un'istruzione Estop. Per gli ingressi locali, gli interruttori di finecorsa 1 e 2 sono impostati sul canale duale complementare per la valutazione dei dati di ingresso provenienti dai due interruttori.

Logica di programma



Sequenza di muting

Di seguito viene descritta la sequenza di muting per questo esempio.

1. Quando l'area pericolosa della macchina è sullo stesso lato dell'operatore, l'interruttore finecorsa N.A. 1 è disattivato e l'interruttore finecorsa N.C. 2 è attivato. Inoltre, la barriera fotoelettrica non è bloccata, pertanto il segnale di abilitazione uscita è attivato. Il segnale di muting 11, relativo al segnale del canale duale complementare per gli interruttori di limite 1 e 2, viene disattivato.

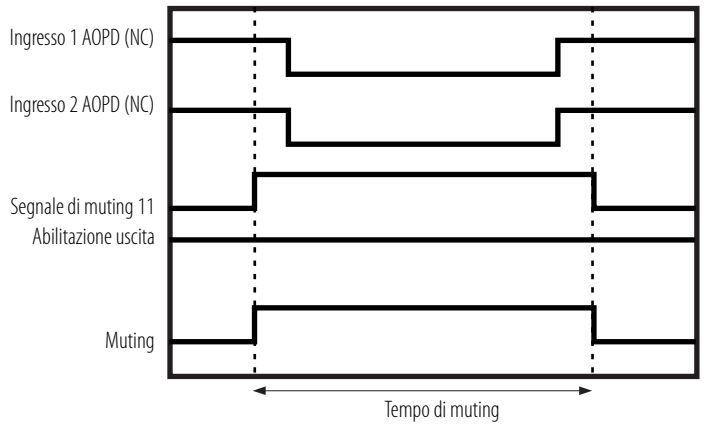
2. Con la rotazione del braccio meccanico, l'interruttore di finecorsa 1 viene attivato e l'interruttore di finecorsa 2 viene disattivato quando l'area pericolosa si trova sul lato opposto all'operatore. Il risultato dell'istruzione Estop, relativo al segnale del canale duale complementare per gli interruttori di finecorsa 1 e 2, viene attivato, pertanto il muting viene abilitato e il segnale di muting attivato.

3. A questo punto, il segnale di abilitazione uscita viene mantenuto attivo anche se la barriera fotoelettrica viene bloccata, in modo che l'operatore possa accedere alla piattaforma di lavoro.

4. Dopo il completamento dell'attività dell'operatore e lo sblocco della barriera fotoelettrica, durante la rotazione del braccio meccanico, il risultato dell'istruzione Estop viene disattivato, lo stato di muting azzerato e il segnale di muting disattivato.

Diagramma dei tempi

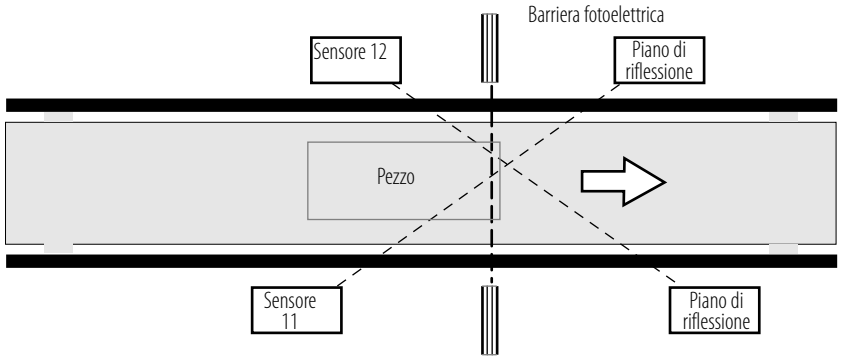
Funzionamento normale



Esempio: funzione di override

La funzione di override può attivare l'uscita di sicurezza anche se il segnale di interruzione del fascio luminoso della barriera fotoelettrica è disattivato. In caso di inceppamento del pezzo durante il transito, il sistema non può tornare al funzionamento normale senza la rimozione forzata del pezzo. In questo caso, è possibile utilizzare la funzione di override per spostare il pezzo all'esterno della zona di rilevamento della barriera fotoelettrica.

Configurazione dell'applicazione



Il sensore 11 è collegato al segnale di muting 11. Il sensore 12 è collegato al segnale di muting 12.

Sequenza di override

Di seguito viene descritta la sequenza di override per il presente esempio.

1. Il segnale di abilitazione uscita è disattivato.

2. Quando gli ingressi di override vengono attivati, la funzione di override viene avviata e il segnale di override attivato. Finché gli ingressi di override restano attivati, lo stato di muting è abilitato in modo forzato e i segnali di muting e di abilitazione uscita sono attivati.

3. Quando il pezzo spostandosi verso destra non viene più rilevato dal sensore (in questo caso, dal sensore 12), lo stato di muting forzato dalla funzione di override viene azzerato e i segnali di muting e di abilitazione uscita vengono disattivati.

Condizioni di avvio override

Se vengono rispettate le seguenti condizioni, la funzione di override viene avviata e i segnali di abilitazione uscita, di muting e di override vengono attivati.

- Almeno un sensore di muting è attivato.
- La barriera fotoelettrica non è attiva (bloccata).
- Il segnale di abilitazione uscita è disattivato.
- Il segnale di ingresso override è attivato (se impostato come ingresso singolo) o attivo (se impostato come ingresso duale).

Condizioni di arresto override

Se una delle seguenti condizioni viene rispettata, la funzione di override viene arrestata e i segnali di muting e di override vengono disattivati.

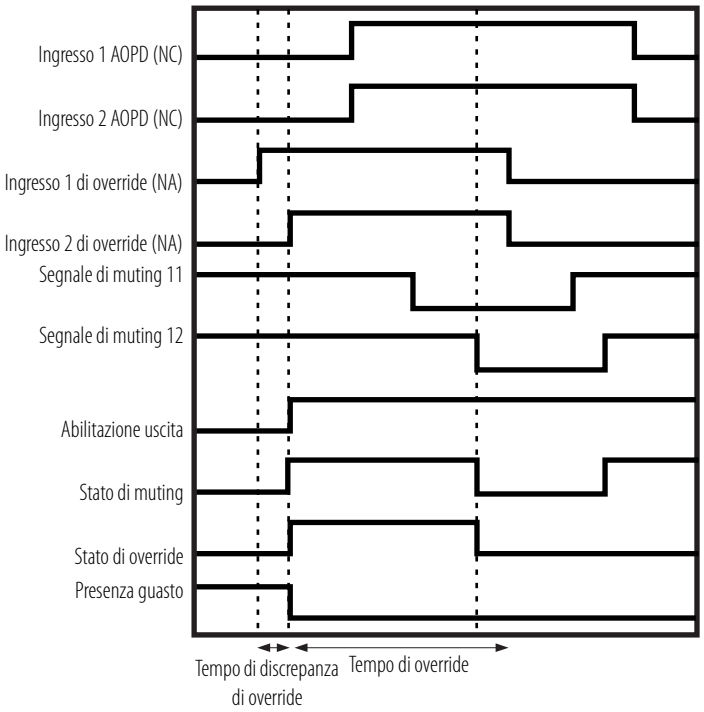
- I segnali di muting sono tutti disattivati.
- Il tempo massimo di override è trascorso.
- Il segnale di ingresso override è disattivato (se impostato come ingresso singolo) o inattivo (se impostato come ingresso duale).

Quando la funzione di override viene arrestata, il segnale di abilitazione uscita viene disattivato se la barriera fotoelettrica è bloccata.

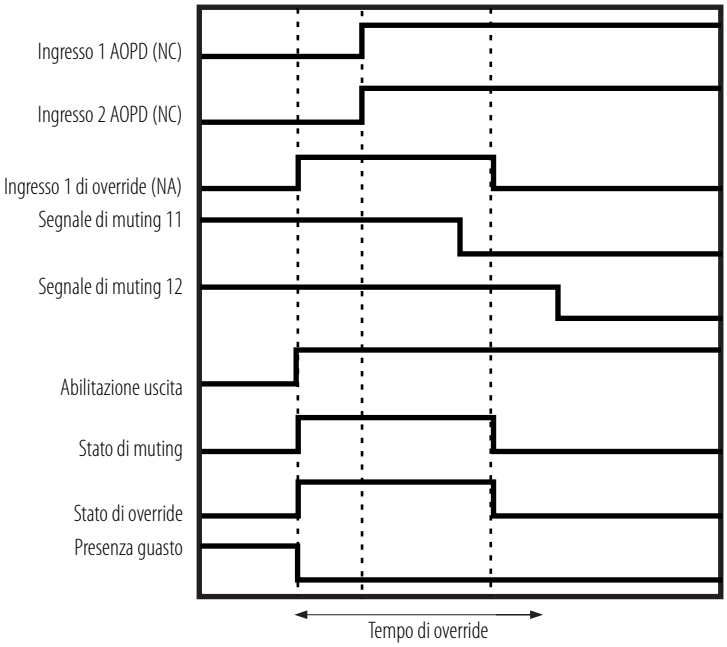
Diagramma dei tempi

Nei seguenti diagrammi viene illustrato il muting parallelo con 2 sensori.

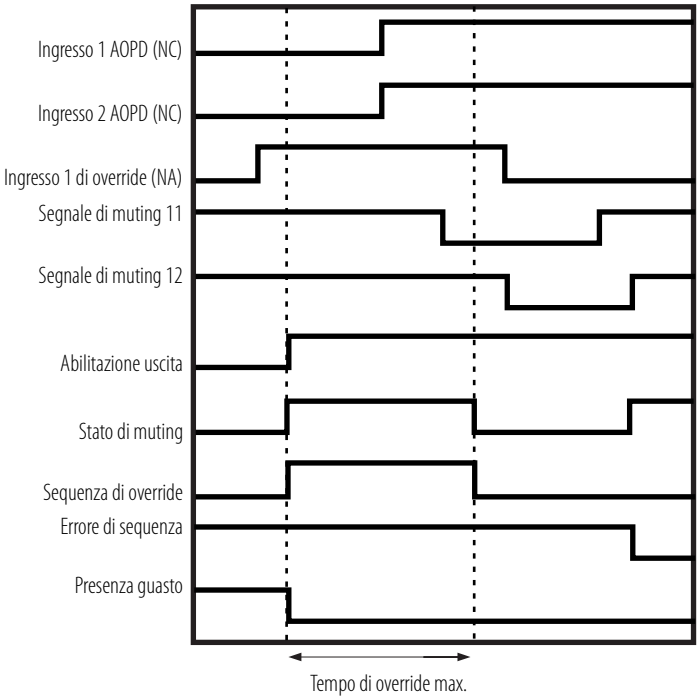
Funzionamento normale della funzione di override



Disattivazione del segnale di override durante l'override

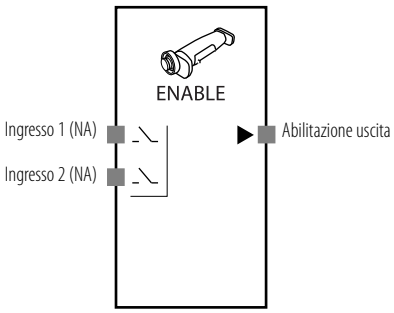


Timeout override durante l'override

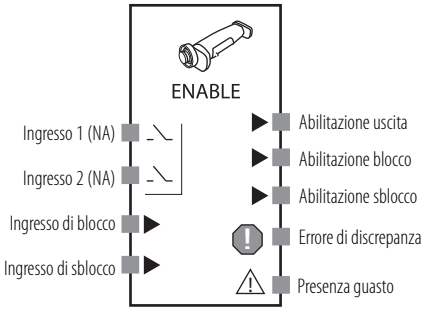


Enable switch

Diagramma del blocco funzione Enable Switch



Connessioni di default



N. massimo di I/O per il blocco funzione Enable Switch

Il blocco funzione Enable Switch consente di monitorare lo stato dell'interruttore di abilitazione. Il segnale di abilitazione uscita viene attivato quando gli ingressi dell'interruttore di abilitazione monitorato sono attivi. Il segnale di abilitazione uscita viene disattivato quando gli ingressi non sono attivi o se viene rilevato un errore nel blocco funzione.

Inoltre, in caso di interruttori di abilitazione che emettono un segnale di blocco e un segnale di sblocco, è possibile monitorare lo stato dei segnali di ingresso di blocco e di ingresso di sblocco del dispositivo. I segnali di ingresso di blocco e di ingresso di sblocco ricevuti non incidono sullo stato del segnale di abilitazione uscita.

Parametri del blocco funzione Enable Switch

Impostare i seguenti parametri per il blocco funzione Enable Switch.

Parametri del blocco funzione Enable Switch

Parametro	Opzioni valide	Impostazione di default
Input Type	Single Channel Dual Channel Equivalent	Doppio canale equivalente
Tempo di discrepanza	Da 0 a 30 s in incrementi di 10 ms.(1) Il tempo di discrepanza deve essere maggiore o uguale alla durata del ciclo del controllore.	30 ms

(1) Il controllo del tempo di discrepanza non viene eseguito se il tempo di discrepanza è impostato su 0.

È possibile portare il numero di ingressi da due a quattro nella scheda In/Out Settings della finestra di dialogo Function Block Properties nel software RSNetWorx for DeviceNet. Sono disponibili due ingressi anche se è stato impostato il canale singolo come tipo di ingresso. È possibile utilizzare i segnali di ingresso di blocco e di ingresso di sblocco quando sono impostati tre o quattro ingressi. L'impostazione di default è due.

Uscite opzionali

Per la programmazione è possibile utilizzare anche le uscite opzionali. Per abilitarle, selezionare le caselle di controllo delle uscite nella scheda Out point della finestra di dialogo Function Block Properties.

- Abilitazione blocco
- Abilitazione sblocco
- Errore di discrepanza

Impostazione dell'uscita Presenza guasto

Nella programmazione è possibile utilizzare anche l'uscita Presenza guasto. Per abilitarla, selezionare la casella di controllo Fault Present nella scheda Out point della finestra di dialogo Function Block Properties.

Gestione degli errori del blocco funzione Enable Switch

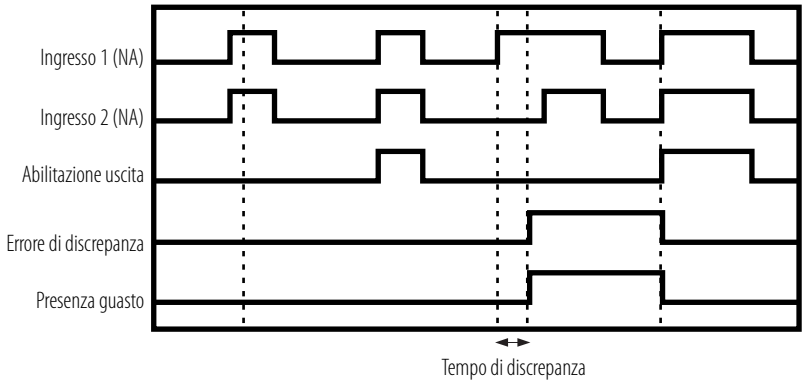
Utilizzare la tabella seguente per individuare e ripristinare una condizione di errore di discrepanza nel blocco funzione Enable Switch.

Rilevamento errori e ripristino per il blocco funzione Enable Switch

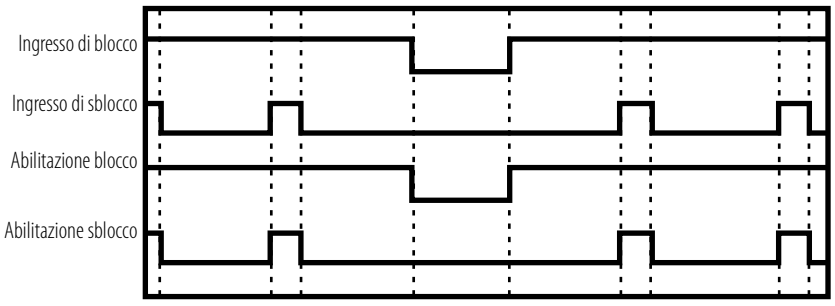
Condizione di errore	Stato al verificarsi dell'errore			Per ripristinare la condizione di errore
	Abilitazione uscita	Presenza guasto	Uscita errore	
Errore di discrepanza per la coppia di ingresso	OFF (Stato di sicurezza)	ON	Errore di discrepanza: ON	Eliminare la causa dell'errore, quindi effettuare una delle operazioni seguenti. 1. Disattivare e riattivare entrambe le coppie di ingresso 1 e 2. 2. modificare la modalità operativa del controllore da riposo a run.

Diagrammi dei tempi del blocco funzione Enable Switch

Funzionamento normale ed errore di discrepanza

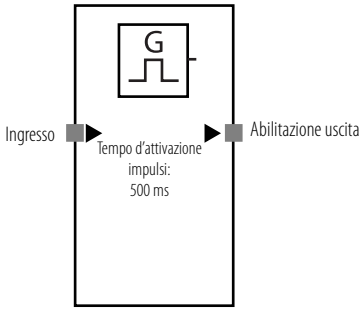


Segnale di blocco e segnale di sblocco



Pulse Generator

Diagramma del blocco funzione Pulse Generator



Il blocco funzione Pulse Generator genera un'uscita a impulsi ON/OFF nel segnale di abilitazione uscita quando il segnale di ingresso del blocco funzione è attivato.

Il tempo di attivazione e disattivazione impulsi può essere impostato in modo indipendente su un valore compreso tra 10 ms e 3 secondi, in incrementi di 10 ms. Se il tempo di attivazione è impostato su 100 ms e il tempo di disattivazione è impostato su 500 ms, il segnale verrà ripetutamente attivato per 100 ms e disattivato per 500 ms.

L'ampiezza dell'impulso di uscita avrà un errore temporale equivalente alla durata del ciclo del controllore SmartGuard. Ad esempio, se la durata del ciclo del controllore SmartGuard è 7 ms e l'ampiezza di impulso è impostata su 100 ms, l'impulso di uscita avrà un valore compreso tra 93 e 107 ms.

Parametri del blocco funzione Pulse Generator

Impostare i seguenti parametri per il blocco funzione Pulse Generator.

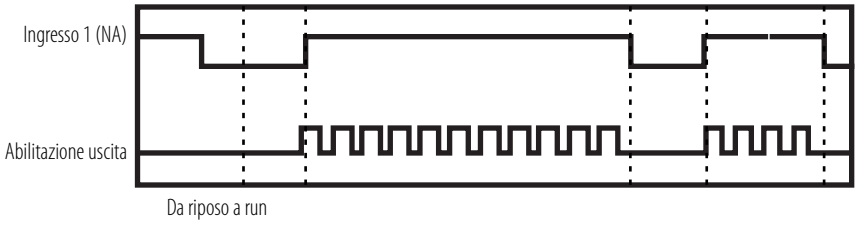
Parametri del blocco funzione Pulse Generator

Parametro	Opzioni valide	Impostazione di default
On pulse time	Da 10 ms a 3 s in incrementi di 10 ms(1)	500 ms
Off pulse time	Da 10 ms a 3 s in incrementi di 10 ms(1)	500 ms

(1) Il valore impostato deve essere superiore alla durata del ciclo del controllore.

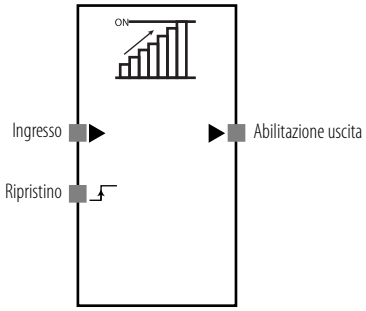
Diagramma dei tempi del blocco funzione Pulse Generator

Diagramma dei tempi Pulse Generator



Counter

Diagramma del blocco funzione Counter



Il blocco funzione Counter conteggia gli impulsi di ingresso in un ingresso e attiva il segnale di abilitazione uscita quando il conteggio raggiunge un valore specifico impostato utilizzando il software RSNetWorx for DeviceNet.

Quando il numero di impulsi in ingresso raggiunge il valore preimpostato, il segnale di abilitazione uscita viene attivato e mantenuto attivo. Per rilevare gli impulsi nel segnale di ingresso, il tempo d'attivazione e di disattivazione dell'impulso di ingresso deve essere superiore alla durata del ciclo del controllore. In caso contrario, potrebbe risultare impossibile rilevare tutti gli impulsi.

Parametri del blocco funzione Counter

Impostare i seguenti parametri per il blocco funzione Counter.

Parametri del blocco funzione Counter

Parametro	Opzioni valide	Impostazione di default
Reset condition	Auto reset Manual reset	Manual reset
Count type	Down counter (decrementing) Up counter (incrementing)	Down counter (decrementing)
Counter	Da 1 a 65.535 conteggi	1

Condizione di ripristino

La condizione di ripristino utilizzata per azzerare il conteggio degli impulsi in ingresso può essere impostata su manuale o automatico. Quando la condizione di ripristino è impostata su automatico e il numero di impulsi in ingresso raggiunge il valore preimpostato, il segnale di abilitazione uscita viene attivato e resta attivo finché il segnale di ingresso è attivo. Quando il segnale di ingresso viene disattivato, il numero di impulsi in ingresso viene azzerato.

Quando la condizione di ripristino è impostata su manuale, il numero di impulsi in ingresso viene azzerato e il segnale di abilitazione uscita viene disattivato quando il ripristino viene attivato. Gli impulsi di ingresso non vengono conteggiati quando il segnale di ripristino è attivo.

Tipo di conteggio

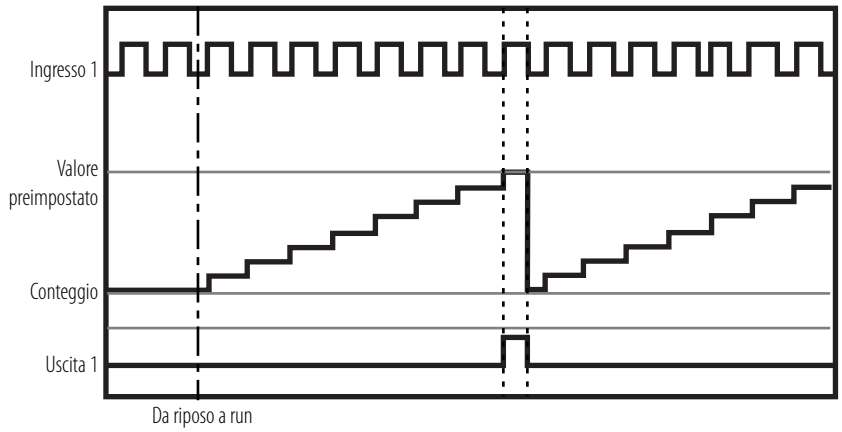
Il tipo di conteggio può essere impostato sul contatore a decremento o sul contatore a incremento.

Con un contatore a decremento, il valore preimpostato rappresenta il valore iniziale del contatore che viene diminuito di una unità ogni volta che viene rilevato un impulso di ingresso. Il segnale di abilitazione uscita viene attivato quando il conteggio raggiunge lo zero. Il valore preimpostato del blocco funzione è memorizzato nell'area di lavoro interna del blocco funzione e può essere monitorato da un dispositivo di programmazione.

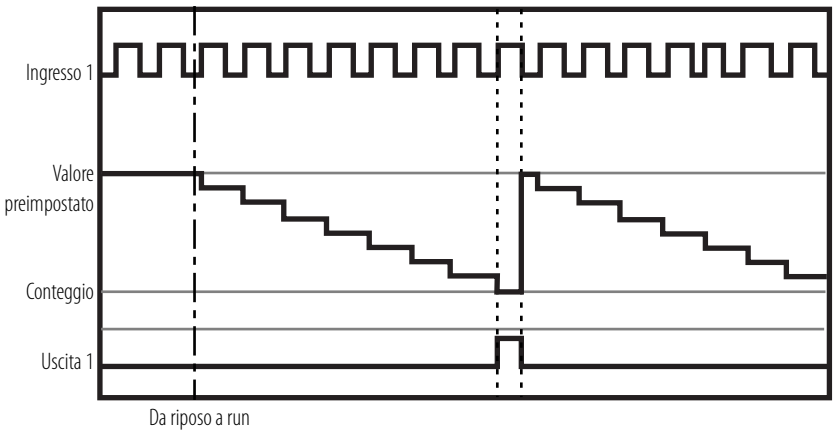
Con un contatore a incremento, il valore iniziale del contatore è zero, valore incrementato di una unità ogni volta che viene rilevato un impulso di ingresso. Il segnale di abilitazione uscita viene attivato quando il conteggio raggiunge il valore preimpostato.

Diagramma dei tempi del blocco funzione Counter

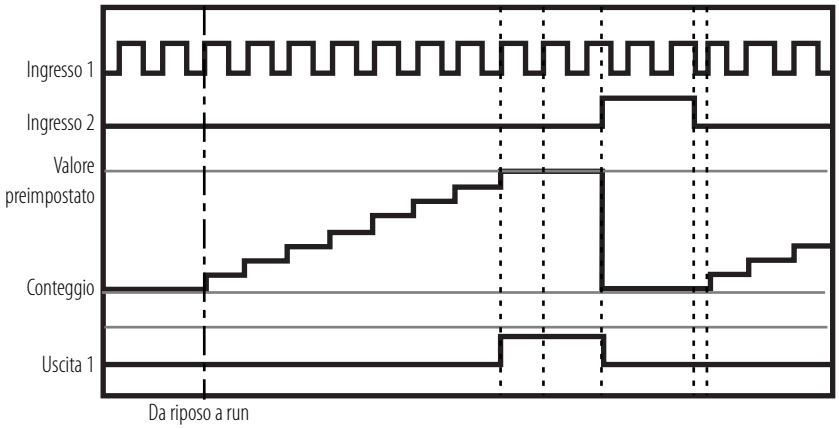
Azzeramento automatico contatore a incremento



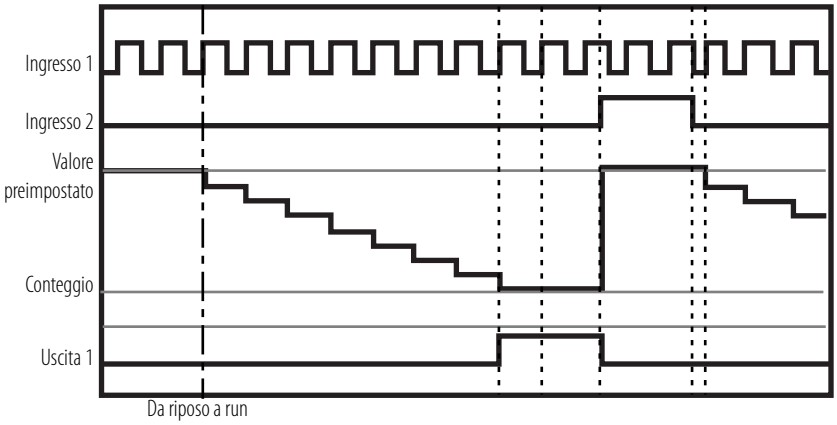
Azzeramento automatico contatore a decremento



Azzeramento manuale contatore a incremento



Azzeramento manuale contatore a decremento



Messaggi espliciti

Introduzione

Argomento	Pagina
Ricezione di messaggi espliciti	271
Invio di messaggi espliciti	274
Accesso ai parametri del controllore utilizzando i messaggi espliciti DeviceNet	276

Ricezione di messaggi espliciti

L'invio di un messaggio esplicito da un master DeviceNet standard a un controllore SmartGuard consente la lettura o la scrittura di tutti i parametri o dati specificati per il controllore SmartGuard. Il controllore esegue un'operazione in base al comando inviato dal master e restituisce una risposta.

Un comando di lettura legge l'I/O locale SmartGuard o l'area I/O slave di sicurezza allocata al controllore SmartGuard dal master.

Di seguito viene riportato il formato di base del comando e della risposta.

Formato del comando

Indirizzo nodo di destinazione	Codice servizio	ID classe		ID istanza		Indirizzo offset		Dimensione dati	
	4B	03	56						

Formato della risposta normale

Numero di byte ricevuti	Indirizzo nodo di origine	Codice servizio	Dati letti						
		CB							

Formato della risposta di errore

Numero di byte ricevuti		Indirizzo nodo di origine	Codice servizio	Codice d'errore	
00	04		94		

Formato del comando

L'Indirizzo nodo di destinazione specifica, in 1 byte esadecimale, l'indirizzo del nodo dei dati da leggere.

Per i comandi, specificare 4B (esadecimale) per il Codice servizio.

L'ID classe è sempre 0356 per i controllori SmartGuard.

L'ID istanza dipende dal tipo di messaggio.

Valori di ID istanza

Tipo di messaggio esplicito	Servizio	ID istanza
Lettura area di ingresso locale	Lettura	0001 (esadecimale)
Lettura area di uscita locale	Lettura	0002 (esadecimale)
Lettura area di ingresso remota di sicurezza	Lettura	0005 (esadecimale)
Lettura area di uscita remota di sicurezza	Lettura	0006 (esadecimale)

I dati di comando includono la dimensione di offset e la dimensione dei dati. La dimensione di offset specifica l'indirizzo da cui iniziare la lettura. Si tratta di un offset in byte dalla prima riga dell'area. La dimensione dei dati specifica il numero di byte da leggere, da 1 a 256. Utilizzare i valori dell'intervallo riportati di seguito come riferimento per l'impostazione dell'offset e delle dimensioni delle varie aree di dati.

Valori dell'intervallo

Area	Intervallo
Area di ingresso locale	0 o 1
Area di uscita locale/test	0 o 1
Area di ingresso remota di sicurezza	0…551
Area di uscita remota di sicurezza	0…551

Formato della risposta

Il Numero di byte ricevuti per le risposte indica il numero di byte di dati ricevuti dall'indirizzo di nodo di origine al termine della risposta restituita (in formato esadecimale).

Il Nodo di origine per le risposte restituisce l'indirizzo del nodo (espresso in 1 byte esadecimale) del controllore SmartGuard che invia la risposta.

Per le risposte, il bit più significativo viene attivato e CB esadecimale viene restituito per il codice servizio.

I Dati letti per le risposte rappresentano i dati I/O restituiti dall'area specificata. Di seguito sono riportati gli offset di indirizzo e le assegnazioni di bit per la lettura degli ingressi locali, delle uscite locali e delle uscite di test. Per questi bit, 1 corrisponde a una condizione normale, mentre 0 indica un errore.

Ingressi locali (2 byte)

Offset (byte)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Morsetto di ingresso di sicurezza numero 7	Morsetto di ingresso di sicurezza numero 6	Morsetto di ingresso di sicurezza numero 5	Morsetto di ingresso di sicurezza numero 4	Morsetto di ingresso di sicurezza numero 3	Morsetto di ingresso di sicurezza numero 2	Morsetto di ingresso di sicurezza numero 1	Morsetto di ingresso di sicurezza numero 0
1	Morsetto di ingresso di sicurezza numero 15	Morsetto di ingresso di sicurezza numero 14	Morsetto di ingresso di sicurezza numero 13	Morsetto di ingresso di sicurezza numero 12	Morsetto di ingresso di sicurezza numero 11	Morsetto di ingresso di sicurezza numero 10	Morsetto di ingresso di sicurezza numero 9	Morsetto di ingresso di sicurezza numero 8

Uscite locali e uscite di test (2 byte)

Offset (byte)	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
0	Morsetto di uscita di sicurezza numero 7	Morsetto di uscita di sicurezza numero 6	Morsetto di uscita di sicurezza numero 5	Morsetto di uscita di sicurezza numero 4	Morsetto di uscita di sicurezza numero 3	Morsetto di uscita di sicurezza numero 2	Morsetto di uscita di sicurezza numero 1	Morsetto di uscita di sicurezza numero 0
1	Riservato				Morsetto di uscita di test numero 3	Morsetto di uscita di test numero 2	Morsetto di uscita di test numero 1	Morsetto di uscita di test numero 0

Formato della risposta di errore

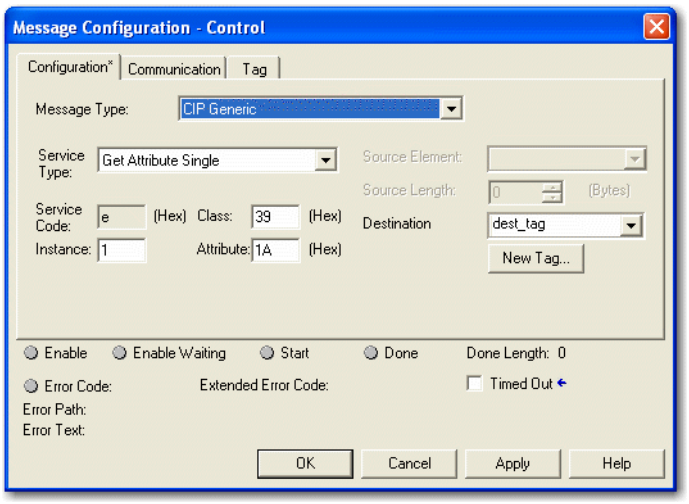
Come la risposta normale, la risposta di errore include il Numero di byte ricevuti, l'Indirizzo nodo di origine e il Codice servizio. Include, inoltre, i codici di errore DeviceNet.

Codici di errore dei messaggi espliciti DeviceNet

Codice risposta	Nome errore	Descrizione
08FF	Servizio non supportato	È presente un errore nel codice servizio.
16FF	L'oggetto non esiste	L'ID istanza specificato non è supportato.
15FF	Troppi dati	I dati hanno una dimensione superiore a quella specificata.
13FF	Dati insufficienti	I dati hanno una dimensione inferiore a quella specificata.
20FF	Parametro non valido	I dati di comando dell'operazione specificata non sono supportati.

Esempio di messaggio di lettura da un controllore GuardLogix

Questa istruzione di messaggio GuardLogix, programmata con il software RSLogix 5000 utilizzando i parametri del formato del comando a pagina 271, legge i dati SmartGuard.



Invio di messaggi espliciti

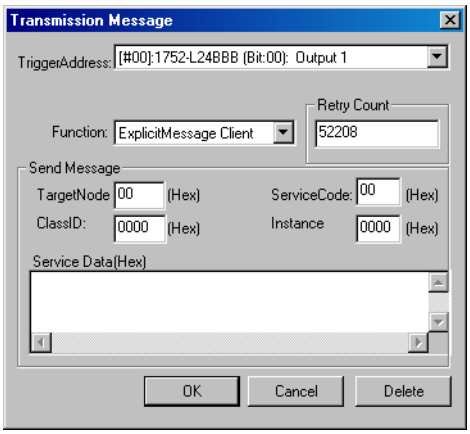
Con i controllori SmartGuard è possibile inviare messaggi espliciti da un programma applicativo dell'utente. I messaggi registrati dall'utente vengono inviati sulla rete quando si verificano le condizioni di attivazione specificate dall'utente. I messaggi possono essere utilizzati per la notifica di dispositivi di controllo e di monitoraggio o come metodo per specificare le uscite per i dispositivi di visualizzazione. È possibile inviare fino a 32 byte di dati di messaggio esplicito.

Formato dei dati dei messaggi espliciti

Nome parametro	Dimensione dati
MAC ID	1 byte
Service Code	1 byte
Class ID	2 byte
Instance ID	2 byte
Service Data	0...26 byte

Attenersi alla seguente procedura per inviare un messaggio esplicito utilizzando lo strumento Logic Editor del software RSNetWorx for DeviceNet.

1. Dalla barra dei menu, selezionare Function > Transmission Message Setting.



2. Utilizzando il menu a discesa TriggerAddress, selezionare il tag di uscita da utilizzare come trigger per l'invio del messaggio esplicito.

   Ogni volta che il tag di uscita specificato passa da disattivato ad attivato, il messaggio esplicito impostato come messaggio da inviare viene inviato.

3. Nel campo Retry Count, immettere il numero di volte per cui tentare l'invio in caso di problemi di trasmissione.

   Immettere 0 per non effettuare altri tentativi.

4. Verificare il formato del messaggio esplicito del nodo di destinazione e creare un messaggio di invio in base alle specifiche del nodo di destinazione, inclusi il nodo di destinazione, il codice servizio, l'ID classe e l'ID istanza.

Restrizioni relative all'invio di messaggi espliciti

I messaggi espliciti sono soggetti alle seguenti restrizioni.

- Nel programma utente è possibile impostare un solo indirizzo di attivazione.
- La memoria I/O interna del controllore SmartGuard viene inviata come risposta a un messaggio esplicito. I messaggi espliciti possono essere inviati da un programma utente del controllore, ma le informazioni interne del controllore non possono essere utilizzate come dati del messaggio da inviare.

- I dati di risposta ai messaggi espliciti non possono essere utilizzati in un programma utente del controllore SmartGuard.

ATTENZIONE

Gli attributi dei dati gestiti dalle comunicazioni I/O standard e dalle comunicazioni tramite messaggi espliciti non sono dati di sicurezza. Durante la generazione dei dati dei messaggi standard o espliciti non vengono adottate le misure necessarie per i dati di sicurezza. Non utilizzare questi dati per gestire un sistema di controllo di sicurezza.

Accesso ai parametri del controllore utilizzando i messaggi espliciti DeviceNet

È possibile leggere i parametri del controllore e scriverli inviando messaggi espliciti DeviceNet al controllore SmartGuard. Il controllore elabora i messaggi ricevuti e restituisce la risposta. I messaggi descritti nelle tabelle seguenti sono supportati dal controllore SmartGuard.

Lettura dello stato generale

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe esad.	ID istanza esad.	ID attributo	Dimensione dati	
Lettura stato generale dell'unità	Lettura	Legge lo stato generale del controllore	0E esad	39 esad	01 esad	6E esad	--	1 byte

Lettura dell'autenticazione di sicurezza

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe esad.	ID istanza esad.	ID attributo	Dimensione dati	
Lettura stato sicurezza dell'unità	Lettura	Legge la marca temporale e l'autenticazione di sicurezza del controllore SmartGuard	0E esad	39 esad	01 esad	1A esad	--	10 byte

Impostazione e monitoraggio dei morsetti di ingresso di sicurezza

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Modalità di monitoraggio per informazioni di manutenzione morsetto	Lettura	Legge la modalità di monitoraggio delle informazioni di manutenzione per l'ingresso (1-16) specificato dall'ID istanza.	0E esad	3D esad	01-10 esad	65 esad	–	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on
	Scrittura	Scrive la modalità di monitoraggio delle informazioni di manutenzione per l'ingresso (1-16) specificato dall'ID istanza.	10 esad	3D esad	01-10 esad	65 esad	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on	
SV per tempo totale di funzionamento o contatore commutazioni off/on dell'ingresso	Lettura	Legge l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'ingresso (1-16) specificato dall'ID istanza.	0E esad	3D esad	01-10 esad	68 esad	–	4 byte 0000 0000 . . . FFFF FFFF esad. (0-4.294.967.295)
	Scrittura	Scrive l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'ingresso (1-16) specificato dall'ID istanza.	10 esad	3D esad	01-10 esad	68 esad	4 byte 0000 0000. . . FFFF FFFF esad. (0-4.294.967.295)	–
Lettura tempo totale di funzionamento o contatore commutazioni off/on dell'ingresso	Lettura	Legge il tempo totale di funzionamento o il contatore commutazioni off/on per l'ingresso (1-16) specificato dall'ID istanza.	0E esad	3D esad	01-10 esad	66 esad	–	4 byte 0000 0000 . . . FFFF FFFF esad. (0-4.294.967.295)
Ripristino tempo totale di funzionamento o contatore commutazioni off/on dell'ingresso	Ripristino	Azzera il tempo totale di funzionamento o il contatore commutazioni off/on per l'ingresso (1-16) specificato dall'ID istanza.	05 esad	3D esad	01-10 esad	66 esad	–	–
Lettura dello stato di monitoraggio tempo totale di funzionamento o contatore commutazioni off/on dell'ingresso	Lettura	Legge lo stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per l'ingresso (1-16) specificato dall'ID istanza.	0E esad	3D esad	01-10 esad	67 esad	–	1 byte 00 esad.: in intervallo 01 esad.: fuori intervallo (oltre il valore di monitoraggio)
Lettura indicatore normale ingresso di sicurezza	Lettura	Legge lo stato dell'indicatore normale del numero (1-16) specificato dall'ID istanza.	0E esad	3D esad	01-10 esad	04 esad	–	1 byte 00 esad.: errore 01 esad.: normale

Impostazione e monitoraggio dei morsetti di ingresso di sicurezza

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Lettura delle informazioni sulla causa dell'errore dell'ingresso di sicurezza	Lettura	Legge la causa dell'indicatore normale del numero (1-16) specificato dall'ID istanza disattivato (errore).	0E esad	3D esad	01-10 esad	6E esad	–	1 byte 00 esad.: nessun errore 01 esad.: configurazione non valida 02 esad: errore segnale di test 03 esad.: errore circuito elettrico interno 04 esad.: errore discrepanza 05 esad.: errore in un altro canale dei canali duali
Lettura AND degli indicatori normali dell'ingresso di sicurezza	Lettura	Legge la causa dell'indicatore normale del numero (1-16) specificato dall'ID istanza disattivato (errore).	0E esad	3E esad	01 esad	05 esad	–	1 byte 00 esad.: errore 01 esad.: tutti normali
Lettura OR dello stato di monitoraggio tempo totale di funzionamento o contatori commutazioni off/on dell'ingresso	Lettura	Legge l'OR dello stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per tutti gli ingressi (1-16).	0E esad		01 esad	72 esad	–	1 byte 00 esad.: tutti i valori nell'intervallo 01 esad.: ingresso fuori intervallo (oltre il valore di monitoraggio)

Impostazione e monitoraggio dei morsetti di uscita di sicurezza

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Modalità di monitoraggio per informazioni di manutenzione morsetto	Lettura	Legge la modalità di monitoraggio delle informazioni di manutenzione per l'uscita (1-8) specificata dall'ID istanza.	0E esad	3B esad	01…08 esad	65 esad	–	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on
	Scrittura	Scrive la modalità di monitoraggio delle informazioni di manutenzione per l'uscita (1-8) specificata dall'ID istanza.	10 esad	3B esad	01…08 esad	65 esad	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on	–
SV per tempo totale di funzionamento o contatore commutazioni off/on dell'uscita	Lettura	Legge l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita (1-8) specificata dall'ID istanza.	0E esad	3B esad	01…08 esad	68 esad	–	4 byte 0000 0000… FFFF FFFF esad. (0-4.294.967.295)
	Scrittura	Scrive l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita (1-8) specificata dall'ID istanza.	10 esad	3B esad	01…08 esad	68 esad	4 byte 0000 0000… FFFF FFFF esad. (0-4.294.967.295)	–
Lettura tempo totale di funzionamento o contatore commutazioni off/on dell'uscita	Lettura	Legge il tempo totale di funzionamento o il contatore commutazioni off/on per l'uscita (1-8) specificata dall'ID istanza.	0E esad	3B esad	01…08 esad	66 esad	–	4 byte 0000 0000… FFFF FFFF esad. (0-4.294.967.295)
Ripristino tempo totale di funzionamento o contatore commutazioni off/on dell'uscita	Ripristino	Azzera il tempo totale di funzionamento o il contatore commutazioni off/on per l'uscita (1-8) specificata dall'ID istanza.	05 esad	3B esad	01…08 esad	66 esad	–	–
Lettura dello stato di monitoraggio tempo totale di funzionamento o contatore commutazioni off/on dell'uscita	Lettura	Legge lo stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita (1-8) specificata dall'ID istanza.	0E esad	3B esad	01…08 esad	67 esad	–	1 byte 00 esad.: in intervallo 01 esad.: fuori intervallo (oltre il valore di monitoraggio)

Impostazione e monitoraggio dei morsetti di uscita di sicurezza

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Lettura indicatore normale dell'uscita di sicurezza	Lettura	Legge lo stato dell'indicatore normale del numero (1-8) specificato dall'ID istanza.	0E esad	3B esad	01…08 esad	05 esad	–	1 byte 00 esad.: errore 01 esad.: normale
Lettura delle informazioni sulla causa dell'errore dell'uscita di sicurezza	Lettura	Legge la causa dell'indicatore normale del numero (1-8) specificato dall'ID istanza disattivato (errore).	0E esad	3B esad	01…08 esad	6E esad	–	1 byte 00 esad.: nessun errore 01 esad.: configurazione non valida 02 esad: rilevamento di sovracorrente 03 esad.: rilevamento cortocircuito 04 esad.: errore costante elevata 05 esad.: errore in uno dei canali duali 06 esad.: errore circuito elettrico relè interno 07 esad.: errore relè 08 esad.: errore dati tra le uscite del canale duale 09 esad.: rilevamento cortocircuito tra cavi
Lettura AND degli indicatori normali dell'uscita di sicurezza	Lettura	Legge la causa dell'indicatore normale del numero (1-8) specificato dall'ID istanza disattivato (errore).	0E esad	3C esad	01 esad	05 esad	–	1 byte 00 esad.: errore 01 esad.: tutti normali
Lettura OR dello stato di monitoraggio tempo totale di funzionamento o contatori commutazioni off/on dell'uscita	Lettura	Legge l'OR dello stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per tutte le uscite (1-8).	0E esad	3C esad	01 esad	72 esad	–	1 byte 00 esad.: tutti i valori nell'intervallo 01 esad.: ingresso fuori intervallo (oltre il valore di monitoraggio)

Monitoraggio dei morsetti di uscita di test

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Modalità di monitoraggio per informazioni di manutenzione morsetto	Lettura	Legge la modalità di monitoraggio delle informazioni di manutenzione per l'uscita di test (1-4) specificata dall'ID istanza.	0E esad	35B esad	01…04 esad	83 esad	–	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on
	Scrittura	Scrive la modalità di monitoraggio delle informazioni di manutenzione per l'uscita di test (1-4) specificata dall'ID istanza.	10 esad	35B esad	01…04 esad	83 esad	1 byte 00 esad.: Modalità tempo totale di funzionamento 01 esad.: Modalità contatore commutazioni off/on	–
SV per tempo totale di funzionamento o contatore commutazioni off/on dell'uscita di test	Lettura	Legge l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita di test (1-4) specificata dall'ID istanza.	0E esad	35B esad	01…04 esad	86 esad	–	4 byte 0000 0000 – FFFF FFFF esad. (0-4.294.967.295)
	Scrittura	Scrive l'SV del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita di test (1-4) specificata dall'ID istanza.	10 esad	35B esad	01…04 esad	86 esad	4 byte 0000 0000… FFFF FFFF esad. (0- 4.294.967.295)	–
Lettura tempo totale di funzionamento o Contatore commutazioni off/on dell'uscita di test	Lettura	Legge il tempo totale di funzionamento o il contatore commutazioni off/on per l'uscita di test (1-4) specificata dall'ID istanza.	0E esad	35B esad	01…04 esad	84 esad	–	4 byte 0000 0000- FFFF FFFF esad. (0-4.294.967.295)
Ripristino tempo totale di funzionamento o contatore commutazioni off/on dell'uscita di test	Ripristino	Azzera il tempo totale di funzionamento o il contatore commutazioni off/on per l'uscita di test (1-4) specificata dall'ID istanza.	05 esad	35B esad	01…04 esad	84 esad	–	–
Lettura dello stato di monitoraggio tempo totale di funzionamento o contatore commutazioni off/on dell'uscita di test	Lettura	Legge lo stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per l'uscita di test (1-4) specificata dall'ID istanza.	0E esad	35B esad	01…04 esad	85 esad	–	1 byte 00 esad.: in intervallo 01 esad.: fuori intervallo (oltre il valore di monitoraggio)

Monitoraggio dei morsetti di uscita di test

Messaggio esplicito	Servizio	Funzione	Comando					Risposta
			Codice servizio	ID classe	ID istanza	ID attributo	Dimensione dati	
Lettura indicatore di sicurezza dell'uscita di test	Lettura	Legge lo stato dell'indicatore di sicurezza per l'uscita di test (1-4) specificata dall'ID istanza.	0E esad	35B esad	01…04 esad	68 esad	–	1 byte 00 esad.: normale 01 esad.: errore
Lettura delle informazioni sulla causa dell'errore dell'uscita di test	Lettura	Legge la causa dell'indicatore normale dell'uscita di test (1-4) specificata dall'ID istanza disattivato (errore).	0E esad	35B esad	01…04 esad	76 esad	–	1 byte 00 esad.: nessun errore 01 esad.: configurazione non valida 02 esad: rilevamento di sovracorrente 05 esad.: errore costante elevata 06 esad.: rilevamento sottocorrente
Lettura OR degli indicatori di sicurezza dell'uscita di test	Lettura	Legge l'OR dell'indicatore di sicurezza per tutte le uscite di test (1-4).	0E esad	35C esad	01 esad	69 esad	–	1 byte 00 esad.: tutti normali 01 esad.: errore
Lettura OR dello stato di monitoraggio tempo totale di funzionamento o contatori commutazioni off/on dell'uscita di test	Lettura	Legge l'OR dello stato di monitoraggio del tempo totale di funzionamento o del contatore commutazioni off/on per tutte le uscite di test (1-4).	0E esad	35C esad	01 esad	72 esad	–	1 byte 00 esad.: tutti i valori nell'intervallo 01 esad.: uscita di test fuori intervallo (oltre il valore di monitoraggio)

Esempi di applicazione e di configurazione

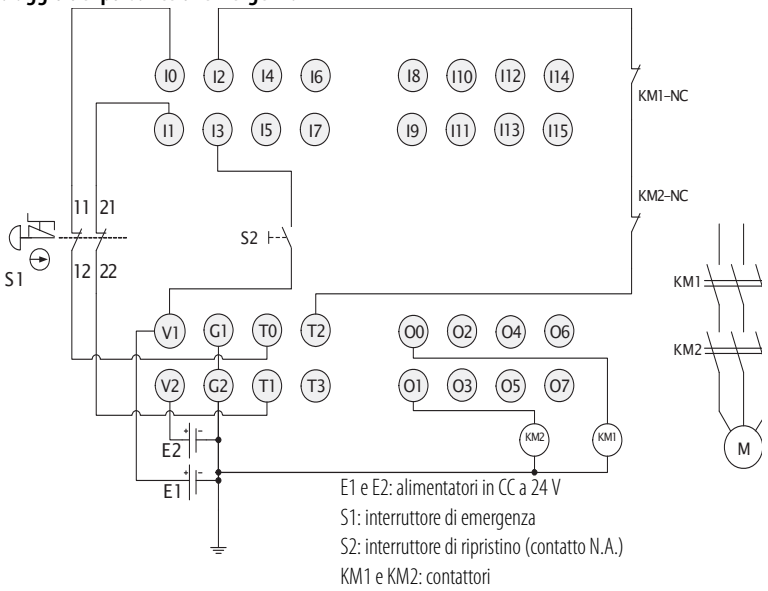
Introduzione

Argomento	Pagina
Applicazione di arresto d'emergenza	283
Applicazione di interblocco di sicurezza con ripristino automatico	285
Applicazione di interblocco di sicurezza a zona duale con interruttore di emergenza con ripristino manuale	286
Applicazione con pedane di sicurezza	288
Applicazione con barriera fotoelettrica	290

Applicazione di arresto d'emergenza

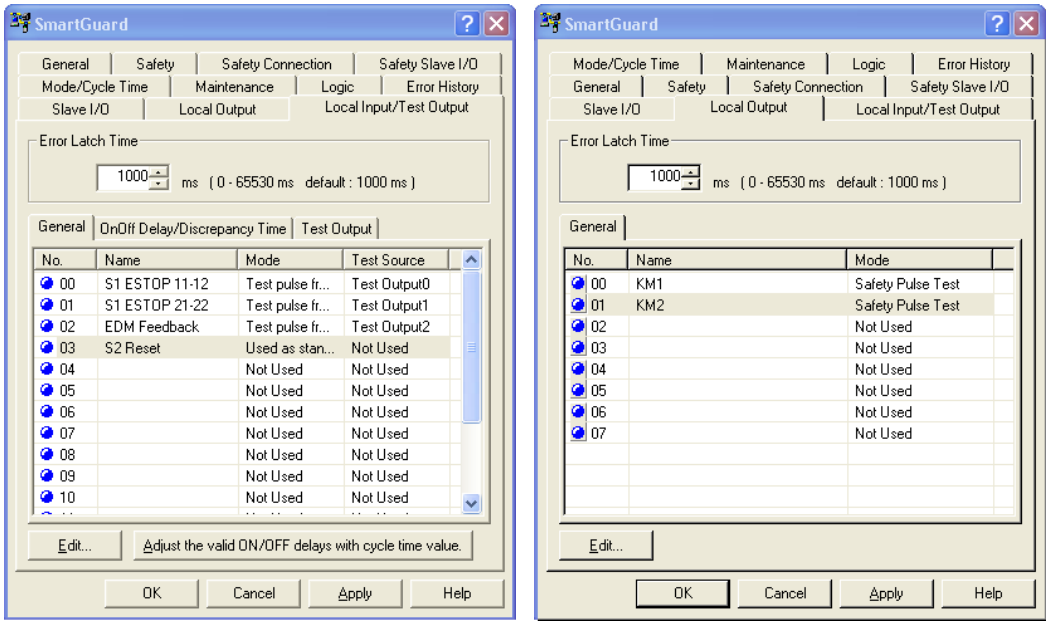
In questo esempio viene illustrato un interruttore di emergenza a canale duale con ripristino manuale.

Schema di cablaggio del pulsante di emergenza



Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione



Programmazione

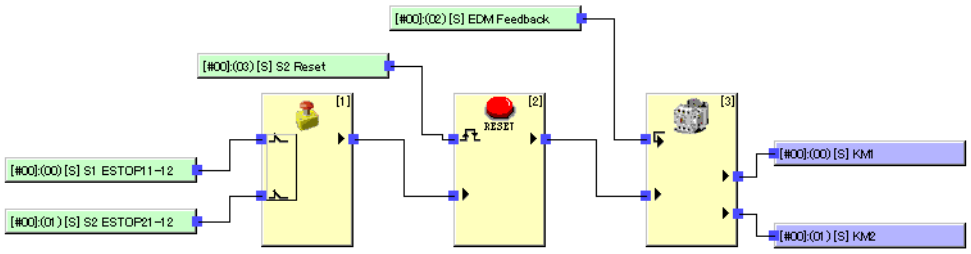
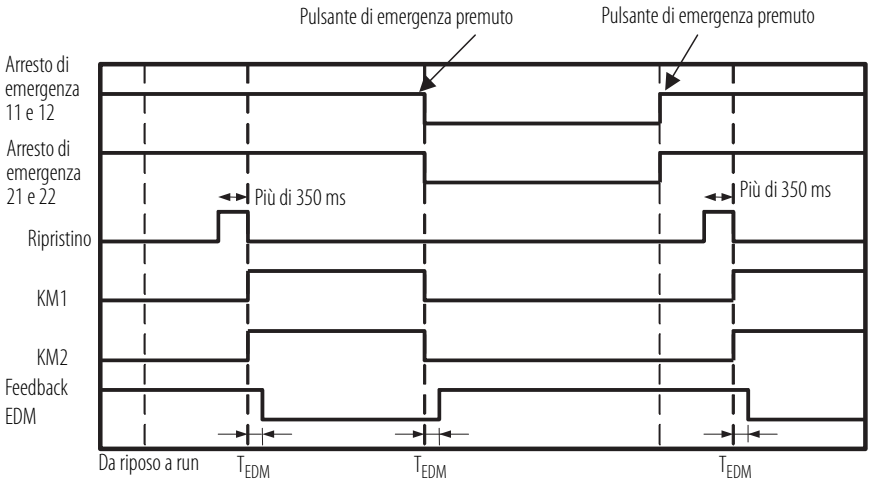


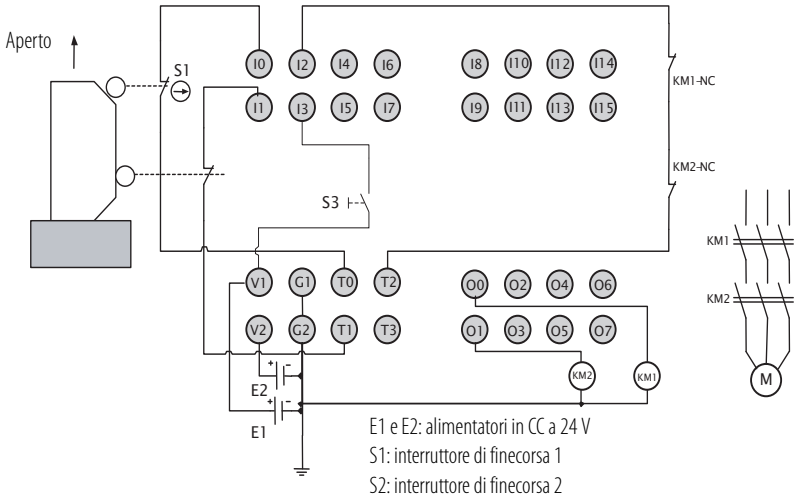
Diagramma dei tempi



Applicazione di interblocco di sicurezza con ripristino automatico

In questo esempio vengono illustrati interruttori di finecorsa a modalità di canale duale con ripristino automatico.

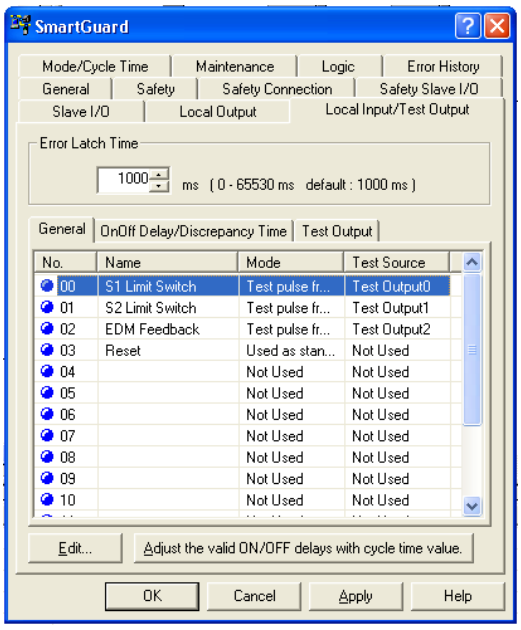
Schema di cablaggio

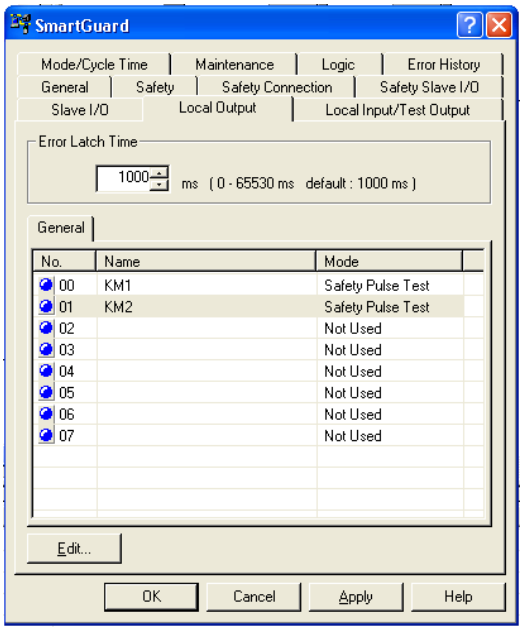


E1 e E2: alimentatori in CC a 24 V
S1: interruttore di finecorsa 1
S2: interruttore di finecorsa 2
S3: interruttore di ripristino
KM1 e KM2: contattori

Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione





Programmazione

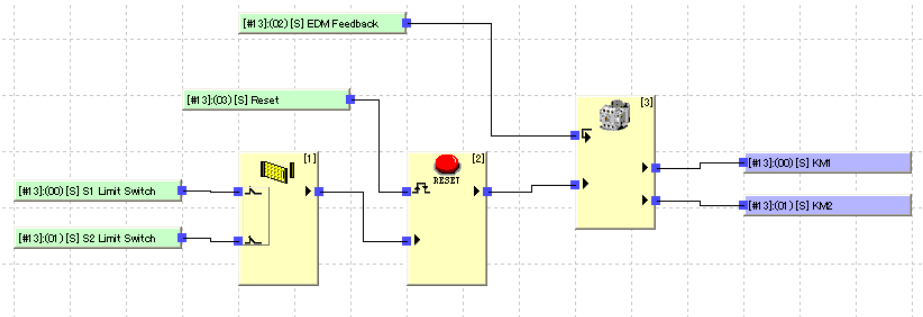
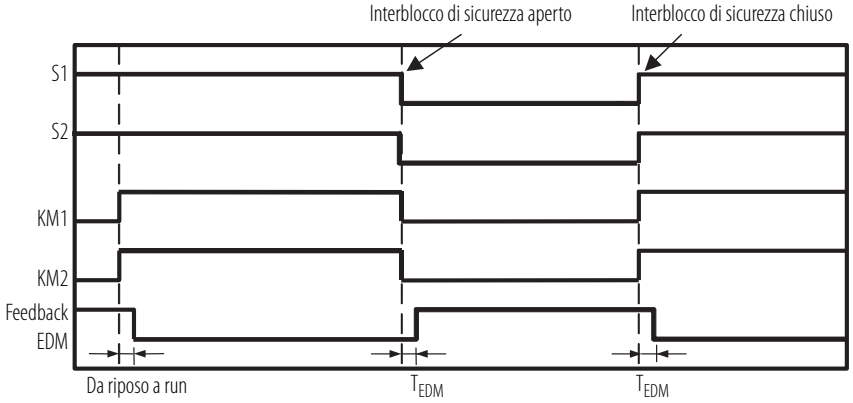


Diagramma dei tempi

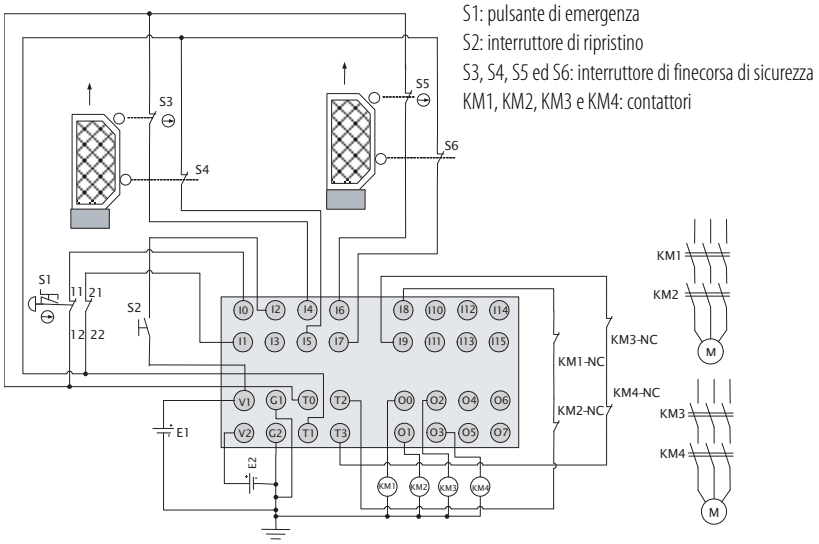


Applicazione di interblocco di sicurezza a zona duale con interruttore di emergenza con ripristino manuale

In questo esempio vengono illustrati interruttori per interblocco a canale duale con ripristino automatico e un interruttore di emergenza a canale duale con ripristino manuale. Ogni coppia di interruttori di interblocco controlla una zona separata in modo tale che una parte della macchina possa continuare a funzionare se il relativo interblocco è chiuso. Il pulsante di emergenza interrompe entrambe le zone.

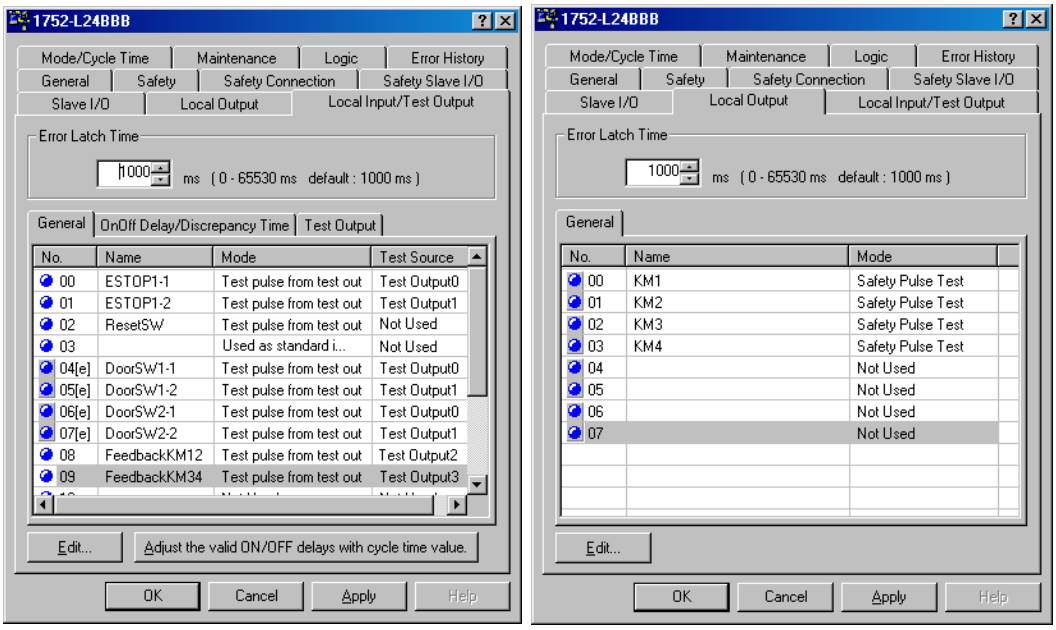
Schema di cablaggio

E1 e E2: alimentatori in CC a 24 V
S1: pulsante di emergenza
S2: interruttore di ripristino
S3, S4, S5 ed S6: interruttore di finecorsa di sicurezza
KM1, KM2, KM3 e KM4: contattori



Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione



Programmazione

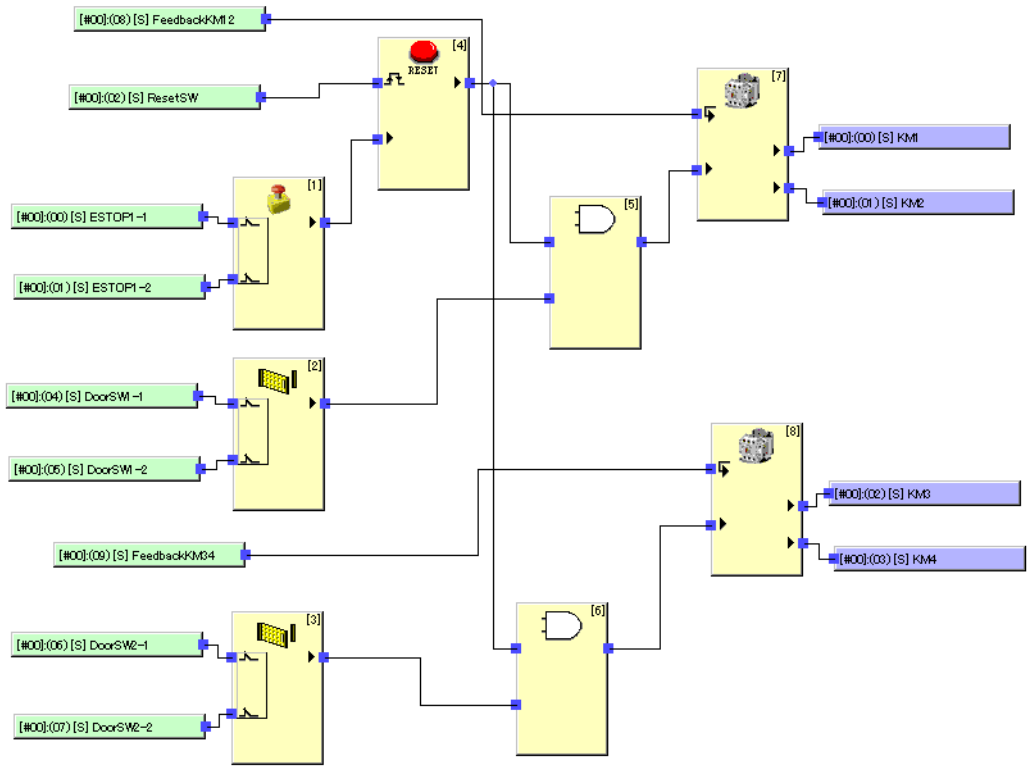
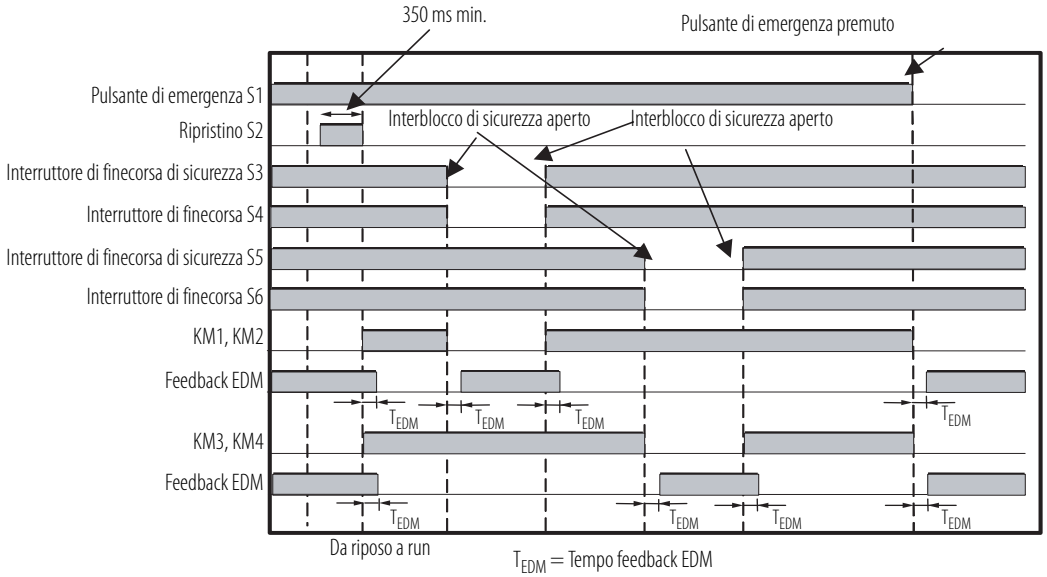


Diagramma dei tempi

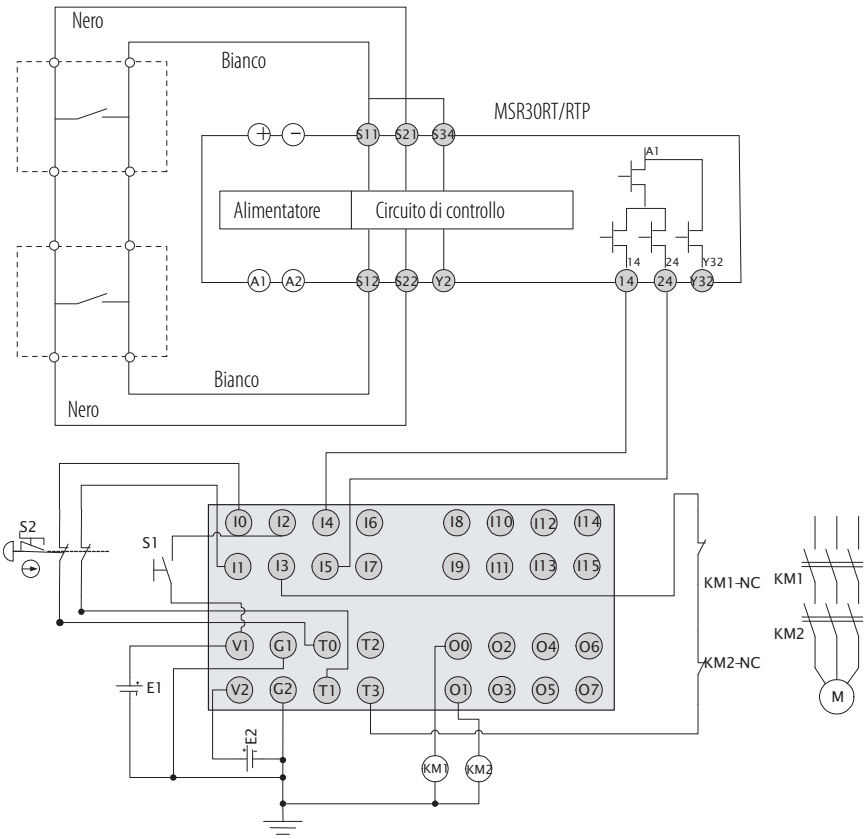


Applicazione con pedane di sicurezza

In questo esempio vengono illustrati una pedana di sicurezza a canale duale con ripristino manuale e un interruttore di emergenza a canale duale con ripristino manuale. L'applicazione utilizza un relè MSR30RT/RTP che dispone di ingressi e uscite a impulsi propri, per cui non viene utilizzata un'uscita di test del controllore SmartGuard.

Schema di cablaggio

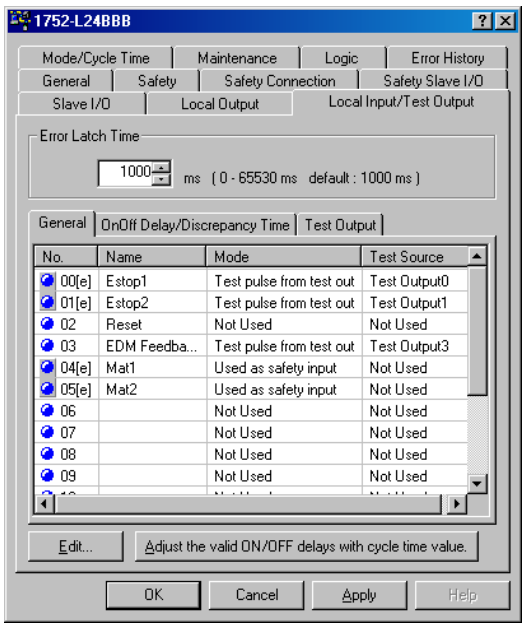
Pedane MatGuard

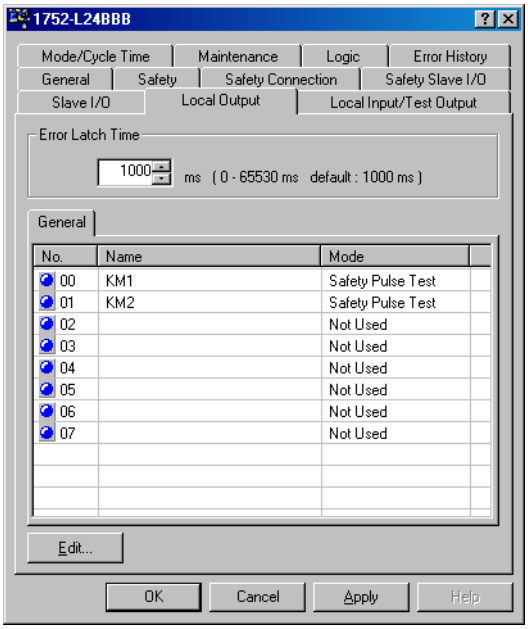


E1 e E2: alimentatori in CC a 24 V
S1: interruttore di ripristino
S2: pulsante di emergenza
KM1 e KM2: contattori

Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione





Programmazione

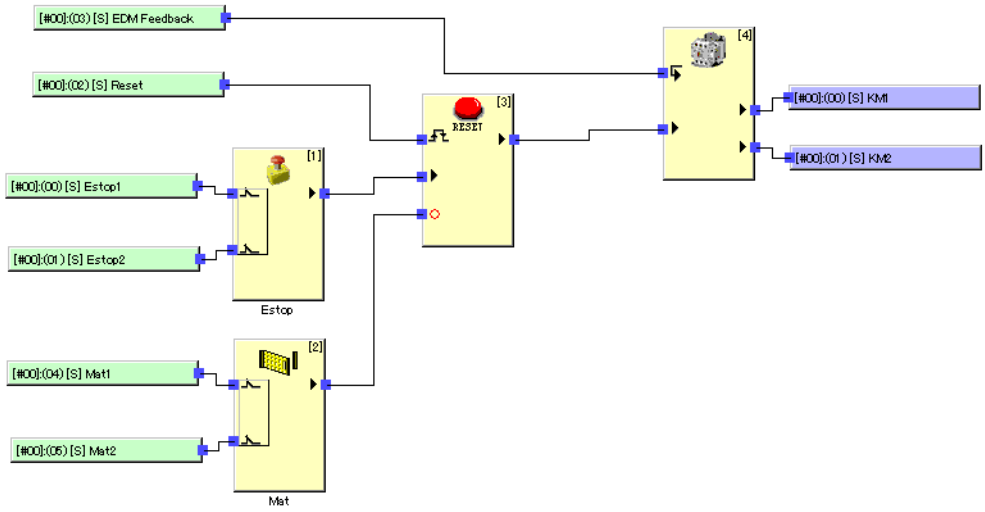
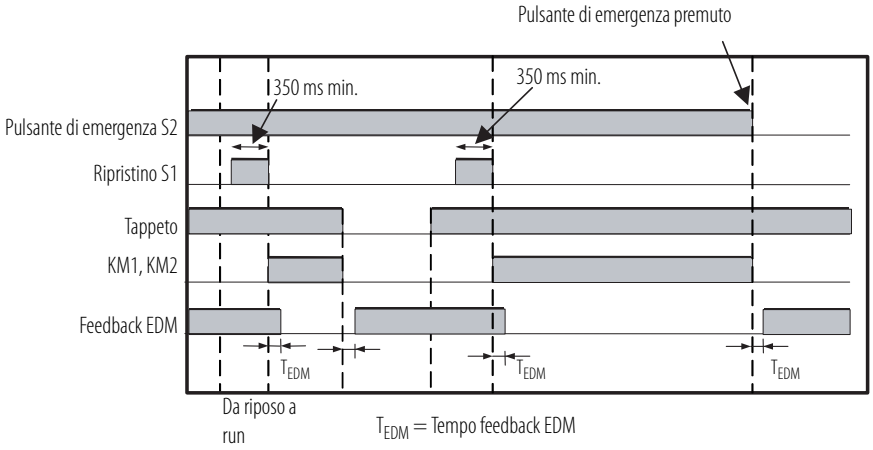


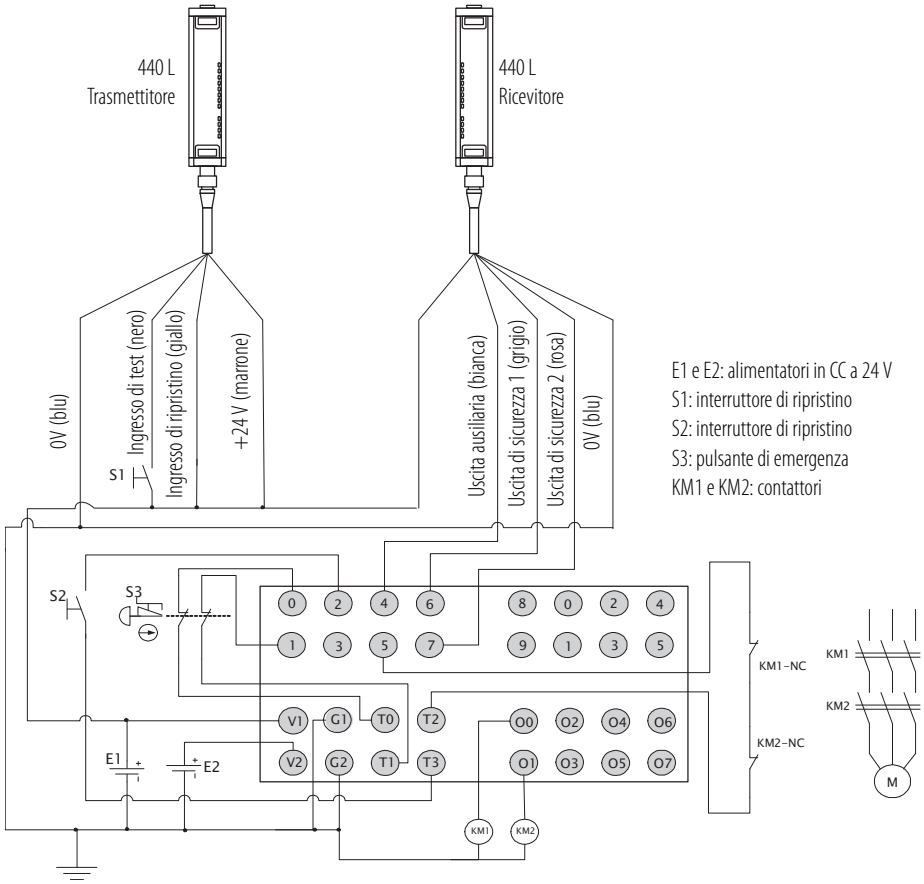
Diagramma dei tempi



Applicazione con barriera fotoelettrica

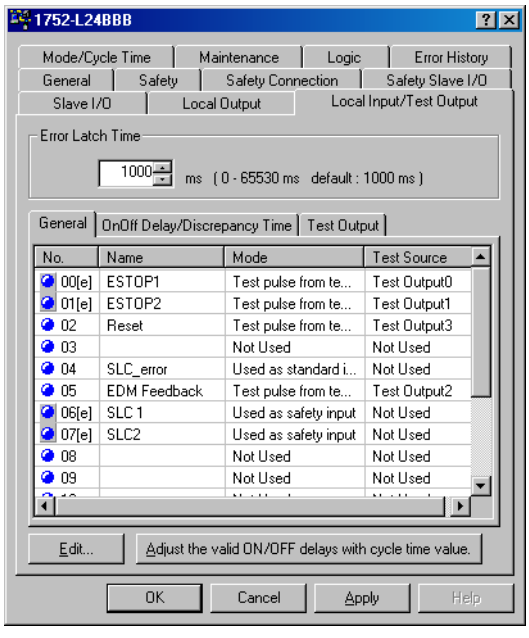
In questo esempio vengono illustrati una barriera fotoelettrica di sicurezza a canale duale con ripristino manuale e un interruttore di emergenza a canale duale con ripristino manuale.

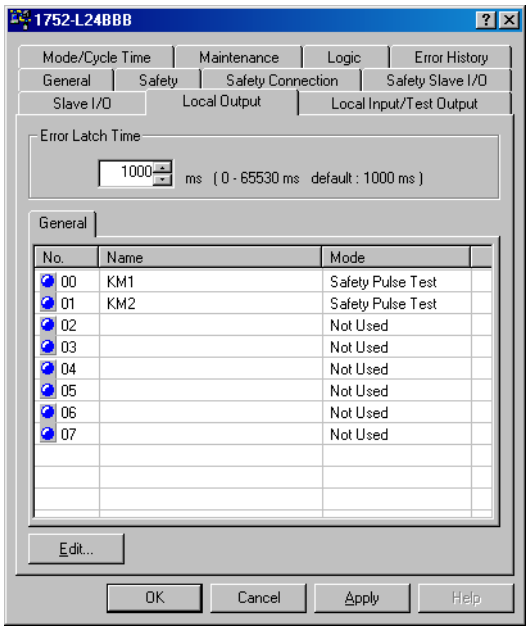
Schema di cablaggio



Collegare un alimentatore in CC 24 V ai morsetti V0 e G0, i morsetti dell'alimentatore per i circuiti interni.

Configurazione





Programmazione

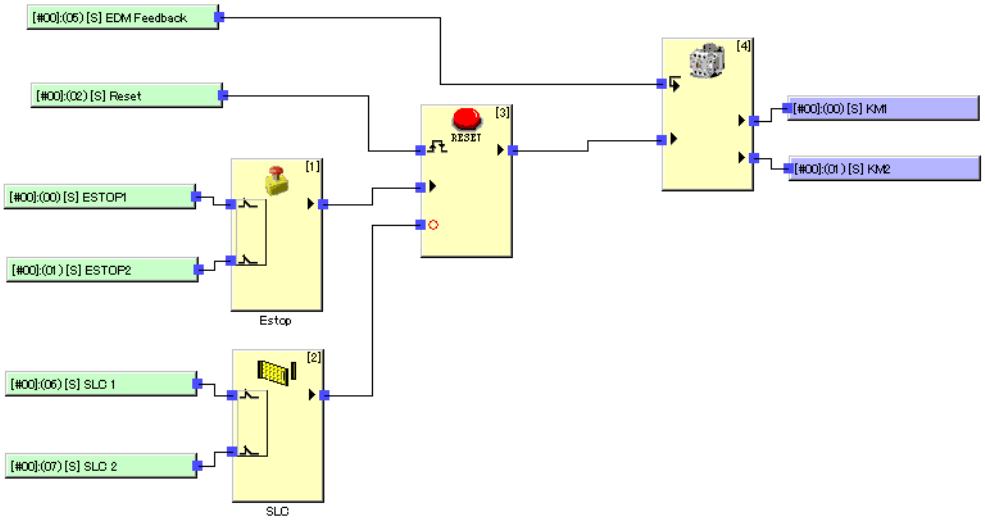
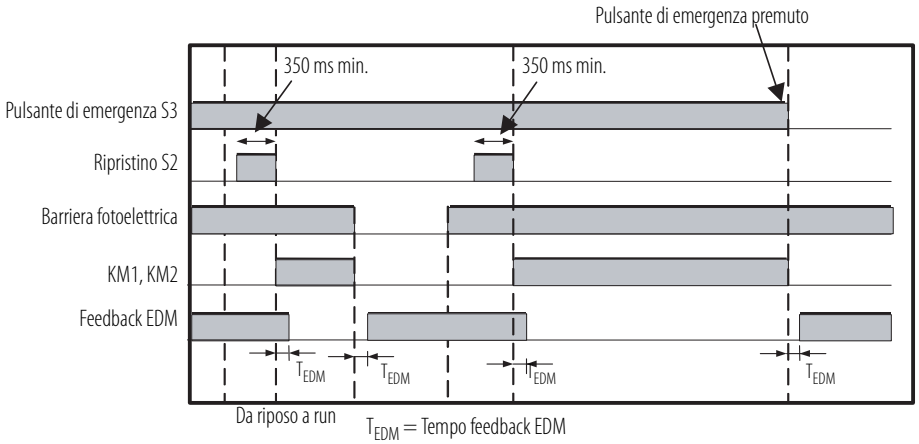


Diagramma dei tempi



Note:

Autenticazione di configurazione

Combinazione di numero ID, data e ora che identificano in modo univoco una configurazione specifica di un dispositivo.

Busoff

Stato che si verifica quando il tasso di errore è estremamente elevato su un cavo di comunicazione. L'errore viene rilevato quando il contatore degli errori interni supera il valore di soglia.

Ciclico

Tipo di comunicazione di dati I/O standard in cui il controllore può inviare e ricevere dati con dispositivi slave che supportano la funzione ciclica. I dati vengono inviati solo alla velocità specificata dall'utente.

Common industrial protocol (CIP)

Protocollo di comunicazione progettato per le applicazioni di automazione industriale.

COS (Change Of State, cambiamento di stato)

Tipo di comunicazione I/O standard in cui il controllore può inviare e ricevere dati con dispositivi slave ogni volta che si verifica una modifica dei dati nel controllore o nel dispositivo slave configurato. I dati vengono aggiornati alla frequenza di heartbeat.

Doppio canale

Utilizzo di due ingressi o uscite come ingresso o uscita per la ridondanza.

Doppio canale complementare

Impostazione per valutare se due stati logici sono complementari.

Doppio canale equivalente

Impostazione per valutare se due stati logici sono equivalenti.

EDS (Electronic Data Sheet, foglio dati elettronico)

Modello fornito dal produttore e utilizzato dal software RSNetWorx for DeviceNet per visualizzare i parametri di configurazione, il profilo di dati I/O e i tipi di collegamenti supportati per un modulo DeviceNet o DeviceNet Safety specifico.

Gruppo

Dati interni di un dispositivo raccolti in gruppo per l'accesso esterno.

I/O di sicurezza

Oltre alla maggior parte degli attributi I/O standard, l'I/O di sicurezza dispone dei meccanismi certificati SIL 3 per la verifica dell'integrità e dell'aggiornamento dei dati.

Impulso di test

Segnale utilizzato per rilevare un contatto tra il cablaggio esterno e l'alimentatore (positivo) o per identificare cortocircuiti tra linee di segnale.

Intervallo di pacchetto richiesto (RPI)

Durante la comunicazione su una rete, rappresenta l'intervallo di tempo previsto per la produzione di dati.

Messaggistica esplicita

Tipo di messaggistica utilizzata per ridurre le attività a priorità più bassa, quali la configurazione e il monitoraggio dello stato.

Nodo

Hardware assegnato a un singolo indirizzo di rete (noto anche come dispositivo o modulo).

Numero della rete di sicurezza (SNN)

Identifica univocamente una rete tra tutte le reti presenti nel sistema di sicurezza. L'utente finale è responsabile dell'assegnazione di un numero univoco ad ogni rete o sottorete di sicurezza presente nel sistema. Il numero della rete di sicurezza fa parte dell'identificatore unico per i nodi (UNID).

PDF (Probabilità di guasto su domanda)

La probabilità media che un sistema operativo non esegua la funzione designata, quando richiesto.

Personal Computer (PC)

Computer utilizzato come interfaccia con un sistema di controllo mediante un software di programmazione.

PFH (Probabilità di guasto all'ora)

La probabilità che in un sistema operativo si verifichino guasti pericolosi in un'ora.

Polling

Tipo di comunicazione di dati I/O standard in cui un messaggio di polling richiede una risposta da un unico dispositivo di rete specifico (un trasferimento di dati punto a punto).

Standard

Qualsiasi oggetto, task, tag, programma o componente di un progetto che non sia un elemento connesso alla sicurezza.

Strobe

Tipo di comunicazione di dati I/O standard in cui un messaggio richiede una risposta da ogni dispositivo (trasferimento multi-cast). Si tratta di un messaggio a 64 bit che contiene 1 bit per ogni dispositivo slave di rete.

Ogni nodo slave può restituire un massimo di 8 byte in risposta all'impulso del master.

Tempo di discrepanza

Periodo di tempo che intercorre tra un cambiamento in uno o due ingressi e il cambiamento dell'altro ingresso.

Tempo di mantenimento dello stato di errore

Periodo di tempo per cui mantenere uno stato di errore (inclusi i relativi dati di controllo, dati di stato e indicazioni di stato).

Tempo di reazione del sistema

Tempo massimo di attesa prima che il sistema passi allo stato di sicurezza dopo un evento correlato alla sicurezza per un ingresso nel sistema o per un errore nel sistema. Il tempo di reazione del sistema include i tempi di reazione dei sensori e degli attuatori e il tempo di reazione del controllore.

Uno di due (1oo2)

Si riferisce alla progettazione funzionale di un sistema di sicurezza a più processori.

Note:

A

Autenticazione di configurazione 45
- Componenti 45
- Confronto 168
- Definizione 45
- Non corrispondente 164

B

Blocco
- Vedere blocco di sicurezza

Blocco di sicurezza
- Dispositivi
- Durante il ripristino 47
- Icona 164

Blocco funzione 71

BOOTP
- Impostazione dell'indirizzo IP 54
- Utilizzo della utility di Rockwell 55

Bridge 59

C

Caratteristiche tecniche
- Generali 195

Caricamento e confronto
- Procedura guidata Safety Device Verification Wizard 166

Categorie di errore 182

Collegamenti multicast 83

Configurazione
- Nodi di destinazione DeviceNet Safety 45
- Parametri di sicurezza 80
- Parametri standard 82
- Ripristino 46
- Verifica 163-169

Configurazione di un driver 42, 52

Connection reaction time limit 84
- E network delay multiplier 85
- Safety I/O DeviceNet 84

D

Dati di stato 177
- Generale 178
- Ingresso locale 179
- Spia di muting 179
- Uscita di test 179
- Uscita locale 179

Display alfanumerico
- Identificazione degli errori 206

Dispositivo mancante
- Icona 164

Dispositivo sconosciuto
- Icona 164

Download della configurazione di DeviceNet 161-162

E

Esempi
- Comunicazione da una rete EtherNet/IP ad una rete DeviceNet 60
- Comunicazione tra rete EtherNet/IP e porta USB 62
- Funzione di bridge 61
- Funzione di bridge di RSLinx 62
- funzione di bridge di RSLinx 60

G

Gateway 53

I

I/O CIP Safety
- Autenticazione di configurazione 45

Icona
- Stato del dispositivo 164

Identificativo di nodo univoco 63

Indicatore di stato rete
- Lampeggiante 202

Indirizzo di nodo 43
- Modifiche 67
- Ripristino 46
- Selezione 26

Indirizzo IP
- Impostazione tramite BOOTP 54
- Impostazione tramite software RSLinx 57
- Panoramica 53

L

Locali
- Ingressi 69-72
- Uscite 76-78

Logica
- Funzioni 143

M

Maschera di sottorete 53
Messa in servizio dei nodi 42-43
Strumento 42
Messaggi di errore
Alimentazione 188
Comunicazione 186
Errori di download 190
Errori di ripristino 192
Guasto del sistema 186
Ingressi di sicurezza 189
Modifica delle modalità 193
Uscite di sicurezza 189
Uscite di test 189
Messaggio esplicito
Invio 274
Restrizioni 275
Ricezione 271
Modalità canale duale
Ingressi 69
Uscite 76
Modulo EtherNet/IP
Funzione di bridge 59
Parametri di configurazione 53

N

Network delay multiplier 85
Non corrispondente
Autenticazione di configurazione 164
SNN 67
Numero della rete di sicurezza 63
Assegnazione 65
Assegnazione automatica 65
Assegnazione manuale 65
Automatico 64
Basato sul tempo 64
Copia 64
Formati 63
Gestione 63
Icona di errore 164
Manuale 64, 65
Non corrispondente 67
Ripristino 46, 67

P

Pagina iniziale 163
Password
Caratteri validi 48
Dimenticata 48
Impostazione o modifica 47
Operazioni protette 47
Ripristino 46, 48
Procedura guidata Safety Device Verification Wizard 47
Avvio 163
Blocco di sicurezza
Caricamento e confronto 166
Definizione 163
Pagina iniziale 163
Report 167
Riepilogo 169
Selezione dei dispositivi 165
Stato del dispositivo 164
Proprietari dei collegamenti di uscita
Ripristino 46
Pubblicazioni correlate 13
Pulsante online 162
Punto a punto 83

R

Ready to be safety locked 167
Ready to be verified 165
Report di verifica
Procedura guidata Safety Device Verification Wizard 167
Report di errore 167
Requested packet interval
E connection reaction time limit 84
E connection reaction time limit
Impostazione 84
Rete
Bridge 59
Rete DeviceNet
Collegamento 41, 51
Configurazione di un driver 42, 52
Rete EtherNet/IP
Collegamento ad un computer 51
Parametri 53

Rilevamento di sovracorrente
Sorgenti di test a impulsi 74
Uscite 76
Ripristino
Attributi di sicurezza 46
Dispositivo di sicurezza 46, 67
Proprietario della configurazione 46
Ripristino di sicurezza 46
Ritardo all'eccitazione 69
Ritardo alla diseccitazione 69
RPI
Vedere Requested packet interval

S

Scanner
Ripristino 67
Scheda dei parametri 82
Scheda per la configurazione della sicurezza 80
Scheda safety connections 83
Software RSLinx
Configurazione dei parametri di rete 57
Funzione di bridge 60, 62
Software RSLogix 5000
Profilo generico software 132
Software RSNetWorx for DeviceNet
Messa in servizio dei nodi 42
Sorgenti di test a impulsi 74
Con gli ingressi 69
Con le uscite 76
Spia di muting
Dati di stato 179
Stato
Indicatori 201
Stato del dispositivo
Procedura guidata Safety Device Verification Wizard 164
Verifica 165

T

Timeout multiplier 85
Tipi di driver 42, 52

U

Utility BOOTP di Rockwell 55

V

Velocità di comunicazione
Ripristino 46
Vedere Velocità di comunicazione
Verifica
Configurazione DeviceNet Safety 163-169
FAILED 167
Selezione dei dispositivi 165
Verify failed 165
Verify not supported 165

Assistenza Rockwell Automation

Rockwell Automation fornisce informazioni tecniche sul Web a supporto dei propri prodotti. All'indirizzo http://support.rockwellautomation.com, è possibile trovare manuali tecnici, risposte a domande frequenti, note tecniche e applicative, codice di esempio, link per scaricare service pack software e la funzione personalizzabile MySupport per l'utilizzo ottimale di questi strumenti.

Per un livello ulteriore di assistenza tecnica telefonica per l'installazione, la configurazione e la ricerca dei guasti, sono disponibili i programmi di assistenza TechConnect. Per ulteriori informazioni, contattare il rappresentante o distributore Rockwell Automation di zona oppure visitare il sito Web http://support.rockwellautomation.com.

Assistenza per l'installazione

Se entro le prime 24 ore dall'installazione viene riscontrato un problema, consultare le informazioni contenute in questo manuale. È anche possibile contattare un numero speciale di assistenza clienti per ottenere il supporto iniziale per configurare e far funzionare il prodotto.

Stati Uniti	1.440.646.3434 Lunedì – Venerdì, dalle 8 alle 17 EST
Altri Paesi	Per qualsiasi problema tecnico, contattare il rappresentante Rockwell Automation di zona.

Restituzione di prodotti nuovi non funzionanti

Tutti i prodotti Rockwell Automation sono sottoposti a rigidi collaudi per verificarne la piena funzionalità prima della commercializzazione. Tuttavia, qualora il prodotto presenti dei malfunzionamenti e debba essere restituito, attenersi alle seguenti procedure.

Stati Uniti	Rivolgersi al proprio distributore. Per completare la procedura di restituzione è necessario fornire al distributore il numero di pratica dell'Assistenza Clienti (per ottenerne uno chiamare i recapiti telefonici sopra riportati).
Altri Paesi	Per la procedura di restituzione, contattare il rappresentante Rockwell Automation di zona.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americhe: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496, USA, Tel: +1 414 382 2000, Fax: +1 414 382 4444
Europa/Medio Oriente/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgio, Tel: +32 2 663 0600, Fax: +32 2 663 0640
Asia: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: +852 2887 4788, Fax: +852 2508 1846

Italia: Rockwell Automation S.r.l., Via Gallarate 215, 20151 Milano, Tel: +39 02 334471, Fax: +39 02 33447701, www.rockwellautomation.it
Svizzera: Rockwell Automation AG, Via Cantonale 27, 6928 Manno, Tel: 091 604 62 62, Fax: 091 604 62 64, Customer Service: Tel: 0848 000 279

Pubblicazione 1752-UM001D-IT-P – Aprile 2009
Copyright © 2009 Rockwell Automation, Inc. Tutti i diritti riservati. Stampato negli U.S.A.